Best practice per gli switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con configurazione e gestione CatOS

Sommario

Informazioni correlate

Introduzione

In questo documento viene descritta l'implementazione degli switch Cisco Catalyst serie 6500/4000, 5500/5000 e 6500/6000 nella rete in uso. Per informazioni sulle configurazioni e i comandi, si presume che sia in esecuzione il software di distribuzione generale Catalyst OS (CatOS) versione 6.4(3) o successive. Sebbene vengano presentate alcune considerazioni di progettazione, questo documento non copre la progettazione complessiva del campus.

Prerequisiti

Requisiti

per la stesura di questo documento, è richiesta la conoscenza della guida di riferimento dei comandi di Catalyst serie 6500, versione 7.6.

Sebbene in tutto il documento siano presenti riferimenti a materiale online pubblico destinato a ulteriore lettura, si tratta di altri riferimenti di base ed educativi:

- Cisco ISP Essentials: caratteristiche essenziali di IOS da tenere in considerazione per ogni ISP.
- Linee guida per il monitoraggio della rete e la correlazione degli eventi Cisco
- Progettazione della rete Gigabit Campus: principi e architettura
- Cisco SAFE: Un progetto di sicurezza per le reti aziendali

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Queste soluzioni rappresentano anni di esperienza sul campo da parte dei tecnici Cisco che lavorano con molti dei nostri clienti più grandi e delle reti complesse. Di conseguenza, in questo documento vengono enfatizzate le configurazioni del mondo reale che rendono le reti efficienti. Questo documento offre le seguenti soluzioni:

- Soluzioni che hanno statisticamente la più ampia esposizione sul campo e quindi il rischio più basso.
- Soluzioni semplici, che offrono una certa flessibilità per risultati deterministici.
- Soluzioni facili da gestire e configurate dai team operativi di rete.
- Soluzioni che promuovono alta disponibilità e alta stabilità.

Il documento si divide in quattro sezioni:

- Configurazione di base: funzionalità utilizzate dalla maggior parte delle reti, quali Spanning Tree Protocol (STP) e trunking.
- Configurazione della gestione: considerazioni sulla progettazione e monitoraggio di sistemi ed eventi tramite SNMP (Simple Network Management Protocol), RMON (monitoraggio da remoto), Syslog, CDP (Cisco Discovery Protocol) e NTP (Network Time Protocol).
- Configurazione della sicurezza: password, sicurezza delle porte, sicurezza fisica e autenticazione tramite TACACS+.
- Elenco di controllo della configurazione: riepilogo dei modelli di configurazione consigliati.

Configurazione di base

In questa sezione vengono descritte le funzionalità implementate con la maggior parte delle reti Catalyst.

Protocolli Catalyst Control Plane

In questa sezione vengono illustrati i protocolli in esecuzione tra gli switch in condizioni operative normali. Una conoscenza di base di questi protocolli è utile per affrontare ogni sezione.

Traffico supervisore

La maggior parte delle funzionalità abilitate in una rete Catalyst richiede la collaborazione di due o più switch, quindi è necessario uno scambio controllato di messaggi keepalive, parametri di configurazione e modifiche di gestione. Che si tratti di protocolli di proprietà di Cisco, come CDP, o basati su standard, come IEEE 802.1d (STP), tutti hanno alcuni elementi in comune quando implementati sulla serie Catalyst.

Nell'inoltro di frame di base, i frame di dati utente hanno origine dai sistemi finali e l'indirizzo di origine e l'indirizzo di destinazione non vengono modificati nei domini a commutazione di layer 2 (L2). Le tabelle di ricerca CAM (Content Addressable Memory) su ciascuno switch Supervisor Engine sono popolate da un processo di apprendimento dell'indirizzo di origine e indicano quale porta di uscita deve inoltrare ogni frame ricevuto. Se il processo di apprendimento degli indirizzi è incompleto (la destinazione è sconosciuta o il frame è destinato a un indirizzo broadcast o multicast), il frame viene inoltrato (propagato) su tutte le porte della VLAN.

Lo switch deve inoltre riconoscere i frame da commutare attraverso il sistema e i frame da indirizzare alla CPU dello switch stessa (nota anche come Network Management Processor [NMP]).

Il control plane Catalyst viene creato utilizzando voci speciali nella tabella CAM, denominate **voci di sistema,** per ricevere e indirizzare il traffico all'NMP su una porta dello switch interna. Pertanto, utilizzando protocolli con indirizzi MAC di destinazione noti, il traffico del control plane può essere separato dal traffico di dati. Eseguire il comando show CAM system su uno switch per confermare questa condizione, come mostrato:

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
```

```
----  -----------------    -----  ----------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco ha un intervallo riservato di indirizzi MAC e di protocollo Ethernet, come mostrato. Ognuna di esse viene illustrata più avanti in questo documento. Tuttavia, nella tabella viene presentato un riepilogo per comodità.

Funzionalità	Tipo di protocollo SNAP HDLC	MAC multicast di destinazione
Protocollo PAgP (Port Aggregation Protocol)	0x0104	01-00-0c-cc-cc-cc
Spanning Tree PVSTP+	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD (Unidirectional Link Detection)	0x0111	01-00-0c-cc-cc-cc
Protocollo Cisco Discovery	0x2000	01-00-0c-cc-cc-cc
DTP (Dynamic Trunking)	0x2004	01-00-0c-cc-cc-cc
STP Uplink Fast	0x200a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1d	N/D - DSAP 42 SAP 42	01-80-c2-00-00-00
ISL (Inter Switch Link)	N/D	01-00-0c-00-00-00
VLAN Trunking (VTP)	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE, 802.3x	N/D - DSAP 81 SAP 80	01-80-C2-00-00-00>0F

La maggior parte dei protocolli di controllo Cisco utilizza un incapsulamento SNAP IEEE 802.3, tra cui **LLC 0xAAAA03, OUI 0x00000C**, che può essere rilevato su una traccia di un analizzatore LAN. Altre proprietà comuni di questi protocolli sono:

- Questi protocolli presuppongono una connettività point-to-point. Notare che l'uso deliberato di indirizzi di destinazione multicast consente a due Catalyst di comunicare in modo trasparente su switch non Cisco, in quanto i dispositivi che non comprendono e intercettano i frame li inondano. Tuttavia, le connessioni point-to-multipoint tramite ambienti multivendor possono causare comportamenti incoerenti e devono in genere essere evitate.
- Questi protocolli terminano sui router di layer 3 (L3); funzionano solo all'interno di un dominio dello switch.
- Questi protocolli ricevono la priorità sui dati utente tramite l'elaborazione e la pianificazione ASIC (Application-Specific Integrated Circuit) in entrata.

Dopo l'introduzione degli indirizzi di destinazione del protocollo di controllo, è necessario descrivere anche l'indirizzo di origine per completezza. I protocolli degli switch utilizzano un indirizzo MAC ricavato da un gruppo di indirizzi disponibili forniti da un EPROM sullo chassis. Usare il comando **show module** per visualizzare gli intervalli di indirizzi disponibili per ciascun modulo quando origina traffico, ad esempio BPDU (Bridge Protocol Data Unit) o frame ISL.

```
>show module

...
Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

La VLAN 1 ha un significato speciale nelle reti Catalyst.

Catalyst Supervisor Engine utilizza sempre la VLAN predefinita, VLAN 1, per contrassegnare una serie di protocolli di controllo e gestione durante il trunking, ad esempio CDP, VTP e PAgP. Per impostazione predefinita, tutte le porte, compresa l'interfaccia sc0 interna, sono configurate come membri della VLAN 1. Tutti i trunk trasportano la VLAN 1 per impostazione predefinita e, nelle versioni software CatOS precedenti alla 5.4, non è stato possibile bloccare i dati utente nella VLAN 1.

Queste definizioni sono necessarie per aiutare a chiarire alcuni termini ben utilizzati nelle reti Catalyst:

- La VLAN di gestione è il luogo in cui risiede sc0; la VLAN può essere modificata.
- La VLAN nativa è definita come la VLAN su cui torna una porta quando non si esegue il trunking e è la VLAN senza tag su un trunk 802.1Q. Per impostazione predefinita, la VLAN 1 è la VLAN nativa.
- Per modificare la VLAN nativa, usare il comando **set vlan** *vlan-id mod/porta*.**Nota:** creare la VLAN prima di impostarla come VLAN nativa del trunk.

Di seguito sono riportati diversi buoni motivi per regolare una rete e modificare il comportamento delle porte nella VLAN 1:

- Quando il diametro della VLAN 1, come di qualsiasi altra VLAN, diventa sufficientemente grande da rappresentare un rischio per la stabilità (in particolare dalla prospettiva di un STP), è necessario ridurlo a zero. Questa condizione viene descritta più dettagliatamente nella sezione Gestione in banda di questo documento.
- I dati del control plane sulla VLAN 1 devono essere tenuti separati dai dati dell'utente per semplificare la risoluzione dei problemi e massimizzare i cicli della CPU disponibili.
- I loop L2 nella VLAN 1 devono essere evitati quando le reti multilivello del campus sono progettate senza STP e, in caso di più VLAN e subnet IP, è ancora necessario il trunking al livello di accesso. A tale scopo, cancellare manualmente la VLAN 1 dalle porte trunk.

In sintesi, annotare le seguenti informazioni sui tronchi:

- Gli aggiornamenti **CDP, VTP e PAgP** vengono sempre inoltrati sui trunk con un tag VLAN 1. Ciò si verifica anche se la VLAN 1 viene eliminata dai trunk e non è la VLAN nativa. Se la

VLAN 1 viene cancellata per i dati utente, ciò non influirà sul traffico del control plane che viene ancora inviato utilizzando la VLAN 1.

- Su un trunk ISL, i pacchetti DTP vengono inviati sulla VLAN1. Ciò si verifica anche se la VLAN 1 viene cancellata dal trunk e non è più la VLAN nativa. Su un trunk 802.1Q, i pacchetti DTP vengono inviati sulla VLAN nativa. In questo caso, anche se la VLAN nativa è stata cancellata dal trunk.
- Nel software PVST+, le **BPDU IEEE 802.1Q** vengono inoltrate senza tag sulla VLAN 1 dello Spanning Tree comune per consentire l'interoperabilità con altri fornitori, a meno che la VLAN 1 non venga cancellata dal trunk. Ciò avviene indipendentemente dalla configurazione VLAN nativa. **Le PVST+** BPDU **Cisco** vengono inviate e contrassegnate per tutte le altre VLAN. Per ulteriori informazioni, consultare la sezione Spanning Tree Protocol in questo documento.
- Le BPDU 802.1s Multiple Spanning Tree (MST) vengono sempre inviate sulla VLAN 1 sui trunk ISL e 802.1Q. Ciò si applica anche quando la VLAN 1 viene eliminata dai trunk.
- Non cancellare o disabilitare la VLAN 1 sui trunk tra i bridge MST e i bridge PVST+. Tuttavia, se la VLAN 1 è disabilitata, il bridge MST deve diventare la radice per consentire a tutte le VLAN di evitare che il bridge MST metta le proprie porte limite in stato di incoerenza radice. per ulteriori informazioni, fare riferimento a Descrizione di Multiple Spanning Tree Protocol (802.1s).

Raccomandazioni

Per mantenere una VLAN in stato **attivo/attivo** senza client o host connessi, è necessario che almeno un dispositivo fisico sia connesso alla VLAN. In caso contrario, la VLAN è in stato **attivo/inattivo**. Al momento, non è disponibile alcun comando per configurare un'interfaccia VLAN **come attiva/attiva** quando non sono presenti porte attive nello switch per quella VLAN.

Se non si desidera connettere un dispositivo, collegare un plug-in di loopback a una porta qualsiasi per la VLAN. In alternativa, provare a utilizzare un cavo crossover che colleghi due porte della VLAN sullo stesso switch. Questo metodo forza la porta verso l'alto. Per ulteriori informazioni, consultare la sezione Loopback Plug in Test di loopback per le linee T1/56K.

Quando una rete è multihomed per i provider di servizi, la rete funge da rete di transito tra due provider di servizi. Se il numero VLAN ricevuto in un pacchetto deve essere convertito o modificato quando passato da un provider di servizi a un altro, è consigliabile usare la funzione QinQ per convertire il numero VLAN.

Protocollo VLAN Trunking

Prima di creare le VLAN, determinare la modalità VTP da usare nella rete. Il VTP consente di apportare modifiche alla configurazione della VLAN a livello centrale su uno o più switch. Le modifiche vengono propagate automaticamente a tutti gli altri switch del dominio.

Panoramica operativa

Il VTP è un protocollo di messaggistica L2 che mantiene la coerenza della configurazione VLAN. Il VTP gestisce l'aggiunta, l'eliminazione e la ridenominazione delle VLAN a livello di rete. Il VTP riduce al minimo gli errori di configurazione e le incoerenze di configurazione che possono causare una serie di problemi, ad esempio nomi VLAN duplicati, specifiche del tipo di VLAN errate e violazioni della sicurezza. Il database VLAN è un file binario e viene memorizzato nella NVRAM

sui server VTP separatamente dal file di configurazione.

Il protocollo VTP comunica tra gli switch utilizzando un indirizzo MAC multicast di destinazione Ethernet (**01-00-0c-cc-cc-cc**) e un protocollo SNAP HDLC di tipo Ox2003. Non funziona sulle porte non trunk (il VTP è un payload di ISL o 802.1Q), quindi i messaggi non possono essere inviati finché il DTP non ha portato online il trunk.

I tipi di messaggi includono annunci riepilogativi ogni cinque minuti, annunci di sottoinsiemi e richieste di annunci quando sono presenti modifiche, e join quando è abilitata l'eliminazione VTP. Il numero di revisione della configurazione VTP viene incrementato di un'unità a ogni modifica apportata a un server, in modo da propagare la nuova tabella in tutto il dominio.

Se si elimina una VLAN, le porte che una volta erano membri di tale VLAN vengono messe in stato inactive. Analogamente, se uno switch in modalità client non è in grado di ricevere la tabella VLAN VTP all'avvio (da un server VTP o da un altro client VTP), tutte le porte nelle VLAN diverse dalla VLAN predefinita 1 vengono disattivate.

Questa tabella fornisce un riepilogo del confronto delle funzioni per diverse modalità VTP:

Funzionalità	Server	Client e	Trasparente	Disattivato[1]
Messaggi VTP di origine	Sì	Sì	No	No
Ascolto dei messaggi VTP	Sì	Sì	No	No
Inoltra messaggi VTP	Sì	Sì	Sì	No
Creazione di VLAN	Sì	No	Sì (solo significativi localmente)	Sì (solo significativi localmente)
Memorizza VLAN	Sì	No	Sì (solo significativi localmente)	Sì (solo significativi localmente)

In modalità VTP `trasparente`, gli aggiornamenti VTP vengono ignorati (l'indirizzo MAC multicast VTP viene rimosso dalla CAM del sistema, che in genere viene utilizzata per selezionare i frame di controllo e indirizzarli al supervisor engine). Poiché il protocollo utilizza un indirizzo multicast, uno switch in modalità trasparente (o uno switch di un altro fornitore) invia semplicemente il frame ad altri switch Cisco del dominio.

[1] Il software CatOS versione 7.1 introduce l'opzione di disabilitare il VTP in modalità `off`. In modalità VTP `off`, lo switch si comporta in modo molto simile alla modalità VTP `trasparente`, con la differenza che la modalità `off` elimina anche l'inoltro degli aggiornamenti VTP.

Questa tabella fornisce un riepilogo della configurazione iniziale.

Funzionalità	Valore predefinito
Nome di dominio VTP	Null
modalità VTP	Server
Versione VTP	La versione 1 è abilitata
Password VTP	Nessuna
Eliminazione VTP	Disattivato

Il VTP versione 2 (VTPv2) include questa flessibilità funzionale. Tuttavia, non è interoperabile con il VTP versione 1 (VTPv1):

- Supporto Token Ring
- Supporto di informazioni VTP non riconosciute; le opzioni ora propagano i valori che non possono analizzare.
- modalità trasparente dipendente dalla versione; `la` modalità `trasparente` non controlla più il nome di dominio. Ciò consente il supporto di più domini in un dominio trasparente.
- propagazione del numero di versione; se il VTPv2 è possibile su tutti gli switch, è possibile abilitare il tutto tramite la configurazione di un singolo switch.

per ulteriori informazioni, fare riferimento a Descrizione e configurazione del protocollo VLAN Trunk Protocol (VTP).

VTP versione 3

Il software CatOS versione 8.1 introduce il supporto per il VTP versione 3 (VTPv3). Il VTPv3 offre miglioramenti rispetto alle versioni esistenti. Questi miglioramenti consentono di:

- Supporto di VLAN estese
- Supporto per la creazione e la pubblicità di VLAN private
- Supporto delle istanze VLAN e delle istanze di propagazione della mappatura MST (supportate in CatOS release 8.3)
- Autenticazione server migliorata
- Protezione dall'inserimento accidentale di un database "errato" in un dominio VTP
- Interazione con VTPv1 e VTPv2
- Possibilità di configurazione per porta

Una delle principali differenze tra l'implementazione del VTPv3 e la versione precedente è l'introduzione di un server primario VTP. In teoria, se il dominio non è partizionato, deve esistere un solo server primario in un dominio VTPv3. Tutte le modifiche apportate al dominio VTP devono essere eseguite sul server primario VTP per poter essere propagate al dominio VTP. In un dominio VTPv3 possono essere presenti più server, noti anche come server secondari. Quando uno switch è configurato come server, per impostazione predefinita diventa un server secondario. Il server secondario può archiviare la configurazione del dominio ma non può modificarla. Un server secondario può diventare il server principale se il trasferimento dallo switch ha esito positivo.

Gli switch con VTPv3 accettano solo un database VTP con un numero di revisione superiore a quello del server primario corrente. Questo processo differisce in modo significativo dal VTPv1 e dal VTPv2, in cui uno switch accetta sempre una configurazione superiore da un router adiacente dello stesso dominio. Questo cambiamento con il VTPv3 fornisce protezione. Se un nuovo switch

viene introdotto nella rete con un numero di revisione VTP superiore, non può sovrascrivere la configurazione VLAN dell'intero dominio.

Il VTPv3 introduce anche un miglioramento alla modalità di gestione delle password da parte del VTP. Se si utilizza l'opzione di configurazione password nascosta per configurare una password come "nascosta", si verificano i seguenti casi:

- La password non viene visualizzata in testo normale nella configurazione. Il formato esadecimale segreto della password viene salvato nella configurazione.
- Se si tenta di configurare lo switch come server primario, viene richiesta la password. Se la password corrisponde a quella segreta, lo switch diventa un server primario, che consente di configurare il dominio.

Nota: è importante notare che il server principale è necessario solo quando si deve modificare la configurazione VTP per una qualsiasi istanza. Un dominio VTP può funzionare senza un server primario attivo perché i server secondari garantiscono la persistenza della configurazione durante i ricaricamenti. Lo stato del server primario viene chiuso per i seguenti motivi:

- A switch reload
- Switchover ad alta disponibilità tra i supervisor engine attivi e ridondanti
- Acquisizione da un altro server
- Una modifica nella configurazione della modalità
- Qualsiasi modifica alla configurazione del dominio VTP, come una modifica in:VersionNome dominioPassword di dominio

Il VTPv3 consente anche agli switch di partecipare a più istanze del VTP. In questo caso, lo stesso switch può essere il server VTP per un'istanza e un client per un'altra istanza, in quanto le modalità VTP sono specifiche di diverse istanze VTP. Ad esempio, uno switch può funzionare in modalità `trasparente` per un'istanza MST mentre lo switch è configurato in modalità `server` per un'istanza VLAN.

In termini di interazione con il VTPv1 e il VTPv2, per impostazione predefinita, in tutte le versioni del VTP le versioni precedenti del VTP eliminano semplicemente gli aggiornamenti della nuova versione. A meno che gli switch VTPv1 e VTPv2 non siano in modalità `trasparente`, tutti gli aggiornamenti VTPv3 vengono scartati. D'altra parte, dopo aver ricevuto un frame VTPv1 o VTPv2 legacy su un trunk, gli switch passano una versione ridotta dell'aggiornamento del database agli switch VTPv1 e VTPv2. Tuttavia, questo scambio di informazioni è unidirezionale in quanto gli switch VTPv1 e VTPv2 non accettano aggiornamenti. Sulle connessioni trunk, gli switch VTPv3 continuano a inviare aggiornamenti ridimensionati e aggiornamenti VTPv3 completi per tenere conto dell'esistenza di router adiacenti VTPv2 e VTPv3 sulle porte trunk.

Per fornire il supporto VTPv3 per le VLAN estese, viene modificato il formato del database VLAN in cui il VTP assegna 70 byte per VLAN. La modifica consente di codificare solo i valori non predefiniti, invece di includere campi non modificati per i protocolli legacy. A causa di questa modifica, il supporto di VLAN 4K è la dimensione del database VLAN risultante.

Suggerimento

Non è consigliabile utilizzare modalità VTP `client/server` o modalità VTP `trasparente`. Alcuni clienti preferiscono la facilità di gestione della modalità `client/server` VTP, nonostante alcune considerazioni annotate in seguito. Si consiglia di disporre di due switch in modalità `server` in ciascun dominio per la ridondanza, in genere i due switch a livello di distribuzione. Gli altri switch del dominio devono essere impostati in modalità `client`. Quando si implementa la modalità

`client/server` con l'uso del VTPv2, tenere presente che un numero di revisione superiore viene sempre accettato nello stesso dominio VTP. Se uno switch configurato in modalità `client` VTP o `server` viene introdotto nel dominio VTP e ha un numero di revisione superiore a quello dei server VTP esistenti, sovrascrive il database VLAN all'interno del dominio VTP. Se la modifica della configurazione non è intenzionale e le VLAN vengono eliminate, la sovrascrittura può causare un'interruzione grave nella rete. Per garantire che gli switch `client` o `server` abbiano sempre un numero di revisione della configurazione inferiore a quello del server, modificare il nome di dominio VTP del client in modo che sia diverso dal nome standard. Quindi ripristina lo standard. Questa azione imposta su 0 la revisione della configurazione nel client.

Il VTP può apportare facilmente delle modifiche in una rete in virtù di vantaggi e svantaggi. Molte aziende preferiscono l'approccio cauto della modalità VTP `trasparente` per le seguenti ragioni:

- Incoraggia l'uso di buone pratiche di controllo delle modifiche, in quanto il requisito per modificare una VLAN su uno switch o su una porta trunk deve essere considerato uno switch alla volta.
- Limita il rischio di un errore dell'amministratore che incida sull'intero dominio, ad esempio l'eliminazione di una VLAN per errore.
- Non vi è alcun rischio che un nuovo switch introdotto nella rete con un numero di revisione VTP superiore possa sovrascrivere l'intera configurazione VLAN di dominio.
- ma è preferibile eliminarle dai trunk in esecuzione sugli switch che non dispongono di porte su tale VLAN. Questo rende il frame flooding più efficiente in termini di larghezza di banda. La potatura manuale è utile anche perché riduce il diametro dello spanning tree (vedere la sezione DTP di questo documento). Prima di eliminare le VLAN non utilizzate sui trunk del canale della porta, verificare che le porte connesse ai telefoni IP siano configurate come porte di accesso con VLAN voce.
- L'intervallo di VLAN esteso in CatOS 6.x e CatOS 7.x, numeri da 1025 a 4094, può essere configurato solo in questo modo. Per ulteriori informazioni, vedere la sezione Riduzione dell'indirizzo MAC e della VLAN estesa in questo documento.
- La modalità VTP `trasparente` è supportata in Campus Manager 3.1, parte di Cisco Works 2000. La vecchia restrizione che richiedeva almeno un server in un dominio VTP è stata rimossa.

Comandi VTP di esempio	Commenti
set vtp domain *name* password *x*	Il CDP controlla i nomi per individuare eventuali cablaggi errati tra i domini. Una password semplice è una precauzione utile contro modifiche non intenzionali. Se si incolla, prestare attenzione ai nomi o agli spazi con distinzione tra maiuscole e minuscole.
impostazione vtp mode transparent	
set	Per switch con porte nella VLAN.

vlan *numero vlan* nome *nome*	
impostazione *mod* trunk*/intervallo vlan porta*	Consente ai trunk di trasportare le VLAN dove necessario - il valore predefinito è tutte le VLAN.
cancella *interval lo vlan mod/porta* trunk	Limita il diametro STP mediante eliminazione manuale, ad esempio sui trunk dal livello di distribuzione al livello di accesso, dove la VLAN non esiste.

Nota: se si specificano le VLAN con il comando **set**, le VLAN vengono aggiunte e non vengono cancellate. Ad esempio, il comando **set trunk x/y 1-10** non imposta l'elenco delle VLAN consentite solo sulle VLAN 1-10. Per ottenere il risultato desiderato, usare il comando **clear trunk x/y 11-1005**.

anche se la commutazione token ring non rientra nell'ambito di questo documento, si noti che la modalità VTP `trasparente` non è consigliata per le reti TR-ISL. La base della commutazione token ring è che l'intero dominio forma un singolo bridge distribuito a più porte, quindi ogni switch deve avere le stesse informazioni VLAN.

Altre opzioni

Il VTPv2 è un requisito fondamentale negli ambienti token ring, in cui è altamente consigliata la modalità `client/server`.

Il VTPv3 consente di implementare un'autenticazione e un controllo della revisione della configurazione più rigorosi. Il VTPv3 fornisce essenzialmente lo stesso livello di funzionalità, ma con una sicurezza più avanzata, offerto dalla modalità `trasparente` VTPv1/VTPv2. Inoltre, il VTPv3 è parzialmente compatibile con le versioni VTP precedenti.

In questo documento vengono illustrati i vantaggi dell'eliminazione delle VLAN per ridurre l'inondazione dei frame non necessaria. Il comando **set vtp pruning enable** elimina automaticamente le VLAN e arresta il flusso inefficiente di frame quando non sono necessarie. A differenza dell'eliminazione manuale delle VLAN, l'eliminazione automatica non limita il diametro dello Spanning Tree.

Da CatOS 5.1, gli switch Catalyst possono mappare i numeri di VLAN 802.1Q superiori a 1000 ai numeri di VLAN ISL. In CatOS 6.x, gli switch Catalyst 6500/6000 supportano 4096 VLAN in conformità allo standard IEEE 802.1Q. Queste VLAN sono organizzate in tre intervalli, solo alcuni dei quali vengono propagati ad altri switch nella rete con VTP:

- VLAN di intervallo normale: 1–1001

- VLAN dell'intervallo esteso: 1025-4094 (può essere propagato solo dal VTPv3)
- VLAN dell'intervallo riservato: 0, 1002—1024, 4095

L'IEEE ha prodotto un'architettura basata su standard per ottenere risultati simili al VTP. In qualità di membro del protocollo GARP (Generic Attribute Registration Protocol) 802.1Q, il protocollo GVRP (Generic VLAN Registration Protocol) consente l'interoperabilità della gestione delle VLAN tra fornitori, ma non rientra nell'ambito di questo documento.

Nota: CatOS 7.x introduce l'opzione di impostare il VTP sulla modalità `off`, una modalità molto simile a `transparent`. Tuttavia, lo switch non inoltra i frame VTP. Ciò può essere utile in alcuni progetti quando si esegue il trunking su switch al di fuori del controllo amministrativo.

Riduzione dell'indirizzo MAC e della VLAN estesa

La funzione di riduzione dell'indirizzo MAC consente l'identificazione di VLAN dell'intervallo esteso. L'abilitazione della riduzione degli indirizzi MAC disabilita il pool di indirizzi MAC utilizzati per lo Spanning Tree VLAN e lascia un singolo indirizzo MAC. Questo indirizzo MAC identifica lo switch. Il software CatOS versione 6.1(1) introduce il supporto della riduzione degli indirizzi MAC per gli switch Catalyst 6500/6000 e Catalyst 4500/4000, in modo da supportare le VLAN 4096 in conformità allo standard IEEE 802.1Q.

Panoramica delle operazioni

I protocolli degli switch utilizzano un indirizzo MAC ricavato da un gruppo di indirizzi disponibili fornito da un EPROM sullo chassis come parte degli identificatori di bridge per le VLAN in esecuzione in PVST+. Gli switch Catalyst 6500/6000 e Catalyst 4500/4000 supportano sia l'indirizzo MAC 1024 che 64, a seconda del tipo di chassis.

Gli switch Catalyst con indirizzi MAC 1024 non consentono la riduzione degli indirizzi MAC per impostazione predefinita. Gli indirizzi MAC sono allocati in sequenza. Il primo indirizzo MAC dell'intervallo viene assegnato alla VLAN 1. Il secondo indirizzo MAC dell'intervallo viene assegnato alla VLAN 2 e così via. In questo modo, gli switch possono supportare 1024 VLAN con ciascuna VLAN e usare un identificatore di bridge univoco.

Tipo di chassis	Indirizzo chassis
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	641

[1] La riduzione degli indirizzi MAC è abilitata per impostazione predefinita per gli switch con 64 indirizzi MAC e la funzione non può essere disabilitata.

Per gli switch Catalyst serie 1024 indirizzi MAC, l'abilitazione della riduzione dell'indirizzo MAC

permette al supporto di 4096 VLAN con esecuzione in istanze PVST+ o 16 Multiple Instance STP (MISTP) di avere identificatori univoci senza un aumento del numero di indirizzi MAC richiesti sullo switch. La riduzione degli indirizzi MAC riduce il numero di indirizzi MAC richiesti dall'STP da uno per VLAN o istanza MISTP a uno per switch.

Nella figura viene mostrato che la riduzione degli indirizzi MAC degli identificatori bridge non è abilitata. L'identificatore del bridge è costituito da una priorità del bridge di 2 byte e da un indirizzo MAC di 6 byte:

La riduzione dell'indirizzo MAC modifica la parte dell'identificatore del bridge STP della BPDU. Il campo di priorità a 2 byte originale viene suddiviso in due campi. La divisione determina un campo di priorità del bridge a 4 bit e un'estensione dell'ID di sistema a 12 bit che consente la numerazione delle VLAN da 0 a 4095.

Se la riduzione dell'indirizzo MAC è abilitata sugli switch Catalyst per usare le VLAN dell'intervallo esteso, abilitare la riduzione dell'indirizzo MAC su tutti gli switch dello stesso dominio STP. Questo passaggio è necessario per mantenere coerenti i calcoli radice STP su tutti gli switch. Dopo aver abilitato la riduzione degli indirizzi MAC, la priorità del bridge radice diventa un multiplo di 4096 più l'ID VLAN. Gli switch senza riduzione dell'indirizzo MAC possono rivendicare inavvertitamente la radice perché hanno una granularità più fine nella selezione dell'ID del bridge.

Linee guida per la configurazione

Quando si configura l'intervallo VLAN esteso, è necessario rispettare alcune linee guida. Lo switch può allocare un blocco di VLAN dell'intervallo esteso per scopi interni. Ad esempio, lo switch può allocare le VLAN per le porte indirizzate o i moduli Flex WAN. L'allocazione del blocco di VLAN inizia sempre dalla VLAN 1006 e procede verso l'alto. Se sono presenti VLAN nell'intervallo richiesto dal modulo Flex WAN, tutte le VLAN richieste non vengono allocate perché le VLAN non vengono mai allocate dall'area VLAN utente. Usare il comando show vlan o il comando show vlan summary su uno switch per visualizzare le VLAN interne e assegnate dall'utente.

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- ------------------------------ --------- ------- --------

1    default                        active    7       4/1-48
```

```
!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

Inoltre, prima di usare le VLAN dell'intervallo esteso, è necessario eliminare tutti i mapping 802.1Q-to-ISL esistenti. Inoltre, nelle versioni precedenti al VTPv3, è necessario configurare staticamente la VLAN estesa su ciascuno switch con l'uso della modalità `trasparente` VTP. Per ulteriori informazioni, consultare la sezione *Linee guida per la configurazione delle VLAN dell'intervallo esteso* in Configurazione delle VLAN.

Nota: nel software versione precedente alla 8.1(1), non è possibile configurare il nome della VLAN per le VLAN dell'intervallo esteso. Questa funzionalità è indipendente da qualsiasi versione o modalità VTP.

Suggerimento

Provare a mantenere una configurazione coerente di riduzione degli indirizzi MAC all'interno dello stesso dominio STP. Tuttavia, l'applicazione della riduzione degli indirizzi MAC su tutti i dispositivi di rete può essere impraticabile quando vengono introdotti nuovi chassis con 64 indirizzi MAC nel dominio STP. La riduzione degli indirizzi MAC è abilitata per impostazione predefinita per gli switch con 64 indirizzi MAC e la funzione non può essere disabilitata. Quando due sistemi sono configurati con la stessa priorità spanning-tree, il sistema senza riduzione dell'indirizzo MAC ha una priorità spanning-tree migliore. Per abilitare o disabilitare la riduzione degli indirizzi MAC, eseguire questo comando:

```
set spantree macreduction enable | disable
```

Le VLAN interne vengono allocate in ordine crescente e iniziano dalla VLAN 1006. Per evitare conflitti tra le VLAN utente e le VLAN interne, assegnare le VLAN utente il più vicino possibile alla VLAN 4094. Sugli switch Catalyst 6500 con software di sistema Cisco IOS®, è possibile configurare l'allocazione delle VLAN interne in ordine decrescente. l'equivalente di Command-Line Interface (CLI) per il software CatOS non è ufficialmente supportato.

Negoziazione automatica

Ethernet/Fast Ethernet

La negoziazione automatica è una funzione opzionale dello standard IEEE Fast Ethernet (FE) (802.3u) che consente ai dispositivi di scambiare automaticamente le informazioni sulla **velocità** e sulle capacità **duplex** tramite un collegamento. La negoziazione automatica funziona sul layer 1 (L1) e ha come destinazione le porte del layer di accesso dove **utenti temporanei** come i PC si connettono alla rete.

Panoramica operativa

La causa più comune dei problemi di prestazioni dei collegamenti Ethernet a 10/100 Mbps si verifica quando una porta sul collegamento funziona in modalità half-duplex, mentre l'altra è in modalità full-duplex. Questo si verifica occasionalmente quando una o entrambe le porte in un collegamento vengono resettate e il processo di negoziazione automatica non genera la stessa

configurazione per entrambi i partner del collegamento. Questo si verifica anche quando gli amministratori riconfigurano un partner del collegamento ma non l'altro. I sintomi tipici sono l'aumento della sequenza di controllo dei fotogrammi (FCS), il controllo di ridondanza ciclico (CRC), l'allineamento o i contatori runt sullo switch.

La negoziazione automatica è descritta in dettaglio in questi documenti. Questi documenti includono spiegazioni sul funzionamento della negoziazione automatica e delle opzioni di configurazione.

- Configurazione e risoluzione dei problemi Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation
- Risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst

Un'idea errata comune sulla negoziazione automatica è che è possibile configurare manualmente un partner di collegamento per la modalità full-duplex 100 Mbps e la modalità di negoziazione automatica per la modalità full-duplex con l'altro partner di collegamento. In realtà, un tentativo di eseguire questa operazione determina una mancata corrispondenza del duplex. Questa situazione è dovuta alla negoziazione automatica di un partner del collegamento, alla mancata visualizzazione di parametri di negoziazione automatica dall'altro partner del collegamento e all'impostazione predefinita della modalità half-duplex.

La maggior parte dei moduli Catalyst Ethernet supporta 10/100 Mbps e la modalità half/full-duplex, ma il comando **show port capabilities *mod/porta*** conferma questa condizione.

FEFI

L'indicazione di guasto Far-end (FEFI) protegge le interfacce 100BASE-FX (fibra) e Gigabit, mentre la negoziazione automatica protegge 100BASE-TX (rame) da errori correlati a livello fisico/segnalazione.

Un **guasto all'estremità remota** è un errore nel collegamento che una stazione può rilevare mentre l'altra no, ad esempio un cavo TX scollegato. Nell'esempio, la stazione di invio potrebbe ancora ricevere dati validi e rilevare che il collegamento è buono tramite link-integrator-monitor. Non rileva che la sua trasmissione non viene ricevuta dall'altra stazione. Una stazione 100BASE-FX che rileva un errore remoto può modificare il flusso IDLE trasmesso per inviare uno speciale modello di bit (detto modello FEFI IDLE) per informare il vicino del guasto remoto; il modello FEFI-IDLE attiva successivamente la disabilitazione della porta remota (errdisable). Per ulteriori informazioni sulla protezione dai guasti, consultare la sezione UDLD di questo documento.

FEFI è supportato da questo hardware e dai seguenti moduli:

- Catalyst 5500/5000: WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 e WS-U5539
- Catalyst 6500/6000 e 4500/4000: Tutti i moduli 100BASE-FX e GE

Suggerimento

La configurazione della negoziazione automatica su collegamenti 10/100 o della velocità del codice rigido e del duplex dipende in ultima analisi dal tipo di partner di collegamento o di dispositivo terminale collegato a una porta dello switch Catalyst. La negoziazione automatica tra dispositivi terminali e switch Catalyst in genere funziona correttamente e gli switch Catalyst sono conformi alla specifica IEEE 802.3u. Tuttavia, possono verificarsi problemi quando le schede NIC

o gli switch dei fornitori non sono conformi esattamente. L'incompatibilità hardware e altri problemi possono essere causati anche da funzionalità avanzate specifiche del fornitore, ad esempio l'auto-polarità o l'integrità del cablaggio, che non sono descritte nella specifica IEEE 802.3u per la negoziazione automatica a 10/100 Mbps. Per ulteriori informazioni, fare riferimento al documento sulla comunicazione dei prodotti: Problemi di prestazioni con le schede NIC Intel Pro/1000T che si connettono a CAT4K/6K per un esempio.

Si preveda che in alcune situazioni sarà necessario impostare host, velocità della porta e duplex. In generale, eseguire le seguenti operazioni di risoluzione dei problemi di base:

- Verificare che la negoziazione automatica sia configurata su entrambi i lati del collegamento o che il codice hardware sia configurato su entrambi i lati.
- Per informazioni sulle avvertenze più comuni, consultare le note di rilascio di CatOs.
- Verificare la versione del driver della scheda NIC o del sistema operativo in esecuzione, in quanto spesso è necessario utilizzare il driver o la patch più recente.

Di norma, provare a utilizzare la negoziazione automatica prima per qualsiasi tipo di partner del collegamento. La configurazione della negoziazione automatica per dispositivi temporanei come i notebook offre vantaggi evidenti. Idealmente, la negoziazione automatica funziona bene anche con dispositivi non transitori quali server e workstation fisse o da switch a switch e da switch a router. Per alcune delle ragioni citate, possono sorgere questioni di negoziato. In questi casi, seguire le procedure di risoluzione dei problemi di base descritte nei collegamenti TAC forniti.

Se la velocità della porta è impostata su `auto` su una porta Ethernet 10/100 Mbps, la negoziazione automatica viene eseguita sia per la velocità che per il duplex. Per impostare la porta su auto, eseguire questo comando:

```
set port speed port range auto
!--- This is the default.
```

Se si utilizza l'hardcode della porta, eseguire i seguenti comandi di configurazione:

```
set port speed port range 10 | 100 set port duplex port range full | half
```

In CatOS 8.3 e versioni successive, Cisco ha introdotto la parola chiave opzionale **auto-10-100**. Utilizzare la parola chiave **auto-10-100** sulle porte che supportano velocità di 10/100/1000 Mbps, ma dove la negoziazione automatica a 1000 Mbps non è desiderabile. L'uso della parola chiave **auto-10-100** rende la porta simile a una porta 10/100 Mbps con velocità impostata su **auto**. La velocità e la modalità duplex vengono negoziate solo per le porte a 10/100 Mbps e la velocità a 1000 Mbps non prende parte alla negoziazione.

```
set port speed port_range auto-10-100
```

Altre opzioni

Quando non si utilizza la negoziazione automatica tra gli switch, l'indicazione di errore L1 può anche essere persa per alcuni problemi. È utile utilizzare i protocolli L2 per migliorare il rilevamento degli errori, ad esempio il protocollo UDLD aggressivo.

Gigabit Ethernet

Gigabit Ethernet (GE) dispone di una procedura di negoziazione automatica (IEEE 802.3z) più estesa di quella di 10/100 Mbps Ethernet e viene utilizzata per scambiare parametri di controllo del flusso, informazioni sugli errori remoti e informazioni duplex (anche se le porte GE della serie Catalyst supportano solo la modalità full-duplex).

Nota: 802.3z è stato sostituito da IEEE 802.3:2000 specifiche. Per ulteriori informazioni, fare riferimento al documento sugli standard IEEE per gli standard LAN/MAN di linea: Archivi per ulteriori informazioni.

Panoramica operativa

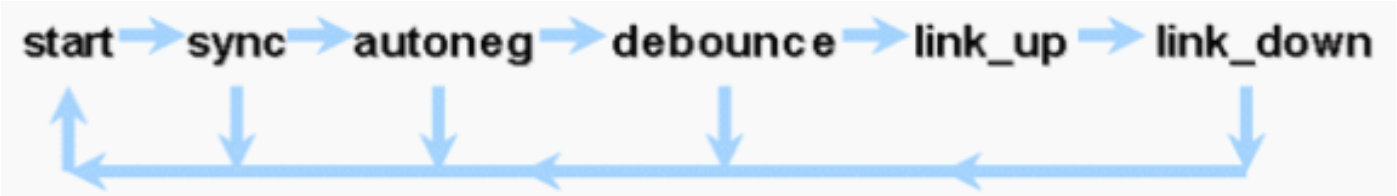
La negoziazione delle porte GE è abilitata per impostazione predefinita e le porte su entrambe le estremità di un collegamento GE devono avere la stessa impostazione. A differenza di FE, il collegamento GE non viene attivato se l'impostazione della negoziazione automatica differisce sulle porte a ciascuna estremità del collegamento. Tuttavia, l'unica condizione necessaria per il collegamento di una porta disabilitata a causa della negoziazione automatica è un segnale Gigabit valido dall'estremità remota. Questo comportamento è indipendente dalla configurazione della negoziazione automatica dell'estremità remota. Si supponga, ad esempio, che vi siano due dispositivi, A e B. Ciascun dispositivo può avere la funzione di negoziazione automatica abilitata o disabilitata. Questa tabella contiene un elenco delle possibili configurazioni e dei rispettivi stati dei collegamenti:

Negoziazione	B abilitato	B Disattivato
A Attivato	`su` su entrambi i lati	A `giù`, B `su`
A Disabilitato	A `su`, B `giù`	`su` su entrambi i lati

In GE, la sincronizzazione e la negoziazione automatica (se abilitate) vengono eseguite all'avvio del collegamento tramite l'utilizzo di una sequenza speciale di parole di codice del collegamento riservate.

Nota: esiste un dizionario di parole valide e non tutte le parole possibili sono valide in GE.

La vita di una connessione GE può essere caratterizzata nel modo seguente:



Una perdita di sincronizzazione indica che l'indirizzo MAC rileva un collegamento non attivo. La perdita della sincronizzazione si verifica indipendentemente dal fatto che la negoziazione automatica sia abilitata o disabilitata. La sincronizzazione viene persa in determinate condizioni non riuscite, ad esempio la ricezione di tre parole non valide in successione. Se questa condizione persiste per 10 ms, viene imposta una condizione di "errore di sincronizzazione" e il collegamento viene impostato sullo stato `link_down`. Una volta persa la sincronizzazione, sono necessari altri tre periodi di inattività validi consecutivi per eseguire nuovamente la sincronizzazione. Altri eventi

catastrofici, come la perdita del segnale di ricezione (Rx), provocano un evento di collegamento non attivo.

La negoziazione automatica fa parte del processo di collegamento. Quando il collegamento è attivo, la negoziazione automatica è terminata. Tuttavia, lo switch continua a monitorare lo stato del collegamento. Se la negoziazione automatica è disabilitata su una porta, la fase "auto-registrazione" non è più un'opzione.

La specifica GE in rame (1000BASE-T) supporta la negoziazione automatica tramite un sistema Next Page Exchange. Next Page Exchange consente la negoziazione automatica per velocità di 10/100/1000 Mbps su porte in rame.

Nota: la specifica della fibra GRE prevede solo la negoziazione del duplex, il controllo del flusso e il rilevamento remoto degli errori. Le porte Fibre Channel GE non negoziano la velocità delle porte. Per ulteriori informazioni sulla negoziazione automatica, fare riferimento alle sezioni 28 e 37 della specifica IEEE 802.3-2002 .

Il ritardo di riavvio della sincronizzazione è una funzionalità software che controlla il tempo totale di negoziazione automatica. Se la negoziazione automatica non ha esito positivo in questo periodo di tempo, il firmware riavvia la negoziazione automatica in caso di deadlock. Il comando **set port sync-restart-delay** ha effetto solo quando la negoziazione automatica è impostata su `enable`.

Suggerimento

L'abilitazione della negoziazione automatica è molto più critica in un ambiente GE che in un ambiente 10/100. In realtà, la negoziazione automatica deve essere disabilitata solo sulle porte dello switch che si connettono a dispositivi che non sono in grado di supportare la negoziazione o laddove problemi di connettività sorgano da problemi di interoperabilità. Cisco consiglia di abilitare la negoziazione Gigabit (predefinita) su tutti i collegamenti da switch a switch e in genere su tutti i dispositivi GE. Per abilitare la negoziazione automatica, eseguire questo comando:

```
set port negotiation port range enable
!--- This is the default.
```

Un'eccezione nota si verifica quando è presente una connessione a un Gigabit Switch Router (GSR) con software Cisco IOS in una versione precedente alla 12.0(10)S, la versione che aggiunge il controllo del flusso e la negoziazione automatica. In questo caso, disattivare le due funzionalità o la porta dello switch `non è connessa` e il GSR segnala gli errori. Di seguito viene riportata una sequenza di comandi di esempio:

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port
negotiation port range disable
```

Le connessioni da switch a server devono essere esaminate caso per caso. I clienti Cisco hanno riscontrato problemi con la negoziazione Gigabit su server Sun, HP e IBM.

Altre opzioni

Il controllo del flusso è una parte opzionale della specifica 802.3x e deve essere negoziato se

utilizzato. I dispositivi possono o non possono inviare e/o rispondere a un frame di pausa (**MAC 01-80-C2-00-00-00 0F noto**). Inoltre, non possono accettare la richiesta di controllo del flusso del vicino più lontano. Una porta con un buffer di input in esaurimento invia un frame di pausa al partner di collegamento, che interrompe la trasmissione e mantiene eventuali frame aggiuntivi nei buffer di output del partner di collegamento. In questo modo non viene risolto alcun problema di sottoscrizione in eccesso allo stato stazionario, ma il buffer di input viene in effetti aumentato di una frazione del buffer di output del partner durante i burst.

Questa funzione è ideale per i collegamenti tra porte di accesso e host finali, dove il buffer di output dell'host è potenzialmente grande quanto la memoria virtuale. L'uso da switch a switch offre vantaggi limitati.

Per controllare questa condizione sulle porte dello switch, eseguire questi comandi:

```
set port flowcontrol mod/port receive | send off |on | desired

>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Nota: tutti i moduli Catalyst rispondono a un frame di pausa se negoziato. Alcuni moduli (ad esempio, WS-X5410 e WS-X4306) non inviano mai frame di pausa anche se negoziano di farlo, in quanto non bloccano.

Dynamic Trunking Protocol

Tipo di incapsulamento

I trunk estendono le VLAN tra i dispositivi identificando e contrassegnando temporaneamente (in locale rispetto al collegamento) i frame Ethernet originali, in modo da consentirne il multiplexing su un singolo collegamento. Ciò garantisce anche il mantenimento del broadcast separato della VLAN e dei domini di sicurezza tra gli switch. Le tabelle CAM mantengono la mappatura frame-to-VLAN all'interno degli switch.

Il trunking è supportato su diversi tipi di supporti L2, tra cui ATM LANE, FDDI 802.10 e Ethernet, sebbene solo quest'ultimo sia presentato qui.

Panoramica operativa ISL

ISL (Cisco Proprietary Identification or Tagging Scheme) è in uso da molti anni. È inoltre disponibile lo standard 802.1Q IEEE.

Incapsulando totalmente il frame originale in uno schema di tagging a due livelli, ISL è effettivamente un protocollo di tunneling e ha il vantaggio aggiuntivo di trasportare frame non Ethernet. Aggiunge un'intestazione da 26 byte e un FCS da 4 byte al frame Ethernet standard - i

frame Ethernet più grandi sono previsti e gestiti dalle porte configurate come trunk. ISL supporta 1024 VLAN.

Formato frame ISL

40 Bit	4 bit	4 bit	48 Bit	16 Bit	24 Bit	24 Bit	15 Bit	Bit	16 Bit	16 Bit	Lunghezza variabile	32 Bit
Dest. Indirizzo	Tipo	UTENTE	SA	LUNGHEZZA	SNAPLLC	HSA	VLAN	BPDU	INDICE	Riserva	Frame incapsulato	FCS
01-00-0c-00-00					AAAA03	000 00C						

Per ulteriori informazioni, fare riferimento a Collegamento tra switch e formato frame IEEE 802.1Q.

Panoramica operativa 802.1Q

Lo standard IEEE 802.1Q specifica molto di più dei tipi di incapsulamento, tra cui i miglioramenti dello Spanning Tree, il GARP (vedere la sezione VTP di questo documento) e il tagging 802.1p Quality of Service (QoS).

Il formato frame 802.1Q mantiene l'indirizzo di origine e l'indirizzo di destinazione Ethernet originali, ma gli switch devono ora aspettarsi di ricevere frame baby-giant, anche sulle porte di accesso dove gli host possono usare la codifica per esprimere la priorità dell'utente 802.1p per la segnalazione QoS. Il tag è di 4 byte, quindi i frame Ethernet v2 802.1Q sono di 1522 byte, un risultato ottenuto dal gruppo di lavoro IEEE 802.3ac. 802.1Q supporta anche la numerazione degli spazi per le VLAN 4096.

Tutti i frame di dati trasmessi e ricevuti sono contrassegnati con lo standard 802.1Q ad eccezione di quelli sulla VLAN nativa (è presente un tag implicito basato sulla configurazione della porta dello switch in entrata). I frame sulla VLAN nativa vengono sempre trasmessi senza tag e ricevuti normalmente senza tag. Tuttavia, possono anche essere ricevuti con tag.

Per ulteriori informazioni, consultare il documento sulla standardizzazione delle VLAN mediante IEEE 802.10 e ottenere IEEE 802 .

Formato frame 802.1Q/801.1p

		Intestazione tag						
		TIPID	TCI					
48 bit	48 bit	16 bit	3 bit	1 bit	12 bit	16 bit	Lunghezz	32 bit

							a variabile	
DA	SA	**TIPID**	**Priority**	**CFI**	**ID VLAN**	Lunghezza/Tipo	Dati con PAD	FCS
		0x8100	**0 - 7**	**0-1**	**0-4095**			

Suggerimento

Poiché tutti i nuovi componenti hardware supportano 802.1Q (e alcuni supportano solo 802.1Q, ad esempio Catalyst serie 4500/4000 e CSS 1000), Cisco consiglia di seguire tutte le nuove implementazioni dello standard IEEE 802.1Q e migrare gradualmente le reti meno recenti da ISL.

Lo standard IEEE consente l'interoperabilità con i fornitori. Ciò è vantaggioso in tutti gli ambienti Cisco in quanto diventano disponibili nuovi dispositivi e schede di interfaccia di rete compatibili con l'host 802.1p. Sebbene entrambe le implementazioni ISL e 802.1Q siano mature, lo standard IEEE avrà alla fine una maggiore esposizione sul campo e un maggiore supporto da parte di terze parti, come il supporto di Network Analyzer. Il minor sovraccarico di incapsulamento di 802.1Q rispetto a ISL è un punto minore a favore anche di 802.1Q.

Poiché il tipo di incapsulamento viene negoziato tra gli switch tramite DTP, con l'ISL scelto come vincitore per impostazione predefinita se entrambe le estremità lo supportano, è necessario usare questo comando per specificare dot1q:

```
set trunk mod/port mode dot1q
```

Se la VLAN 1 viene eliminata da un trunk, come indicato nella sezione Gestione in banda di questo documento, anche se non vengono trasmessi o ricevuti dati utente, il protocollo NMP continua a passare protocolli di controllo come CDP e VTP sulla VLAN 1.

Inoltre, come descritto nella sezione VLAN 1 di questo documento, i pacchetti CDP, VTP e PAgP vengono sempre inviati sulla VLAN 1 quando si esegue il trunking. Quando si utilizza l'incapsulamento dot1q, questi frame di controllo sono contrassegnati con la VLAN 1 se viene modificata la VLAN nativa dello switch. Se il trunking dot1q su un router è abilitato e la VLAN nativa è modificata sullo switch, è necessaria una sottointerfaccia nella VLAN 1 per ricevere i frame CDP contrassegnati e fornire visibilità sui router adiacenti CDP.

Nota: il dot1q può causare problemi di sicurezza causati dalla codifica implicita della VLAN nativa, in quanto è possibile inviare frame da una VLAN a un'altra senza un router. Per ulteriori informazioni, fare riferimento alla sezione Quali sono le vulnerabilità nelle implementazioni VLAN? per ulteriori dettagli. Per ovviare al problema, è possibile usare un ID VLAN per la VLAN nativa del trunk che non sia usato per l'accesso degli utenti finali. La maggior parte dei clienti Cisco lascia la VLAN 1 come VLAN nativa su un trunk e assegna le porte di accesso alle VLAN diverse dalla

VLAN 1 in modo da ottenere questo semplice risultato.

Modalità trunking

Il DTP è la seconda generazione di ISL dinamico (DISL) e viene utilizzato per verificare che i diversi parametri coinvolti nell'invio dei frame ISL o 802.1Q, come il tipo di incapsulamento configurato, la VLAN nativa e la funzionalità hardware, siano concordati dagli switch a una delle estremità del trunk. Ciò contribuisce anche a proteggere le porte non trunk che allagano i frame con tag, un rischio di sicurezza potenzialmente grave, garantendo che le porte e i loro vicini si trovino in stati coerenti.

Panoramica operativa

Il DTP è un protocollo L2 che negozia i parametri di configurazione tra una porta dello switch e la porta adiacente. Utilizza un altro indirizzo MAC multicast (**01-00-0c-cc-cc-cc**) e un tipo di protocollo SNAP 0x2004. La tabella seguente è un riepilogo delle modalità di configurazione:

Modalità	**Funzione**	**Frame DTP trasmessi**	**Stato finale (porta locale)**
`Automatico (impostazione predefinita)`	Rende la porta disponibile a convertire il collegamento in trunk. La porta diventa una porta trunk se la porta adiacente è impostata `sulla` modalità `accesa` o `desiderata`.	Sì, periodico.	Trunking
`On`	Imposta la porta in modalità trunking permanente e negozia per convertire il collegamento in trunk. La porta diventa una porta trunk anche se la porta adiacente non accetta la modifica.	Sì, periodico.	Trunking, **incondizionatamente**.
`Nonegotiate`	Porta in modalità	No	Trunking, **incondiziona**

	trunking permanente ma impedisce alla porta di generare frame DTP. È necessario configurare manualmente la porta adiacente come porta trunk per stabilire un collegamento trunk. Questa opzione è utile per i dispositivi che non supportano il DTP.		**tamente**.
`Desirable`	Fa in modo che la porta tenti attivamente di convertire il collegamento in un collegamento trunk. La porta diventa una porta trunk se la porta adiacente è impostata `su on`, `desired` o `auto` mode.	Sì, periodico.	La modalità termina con il trunking solo se la modalità remota è `attivata`, `automatica` o `desiderabile`.
`Spento`	Porta in modalità non trunking permanente e negozia per convertire il collegamento in un collegamento non trunk. La porta diventa una porta non trunk anche se la porta adiacente non	No nello stato stazionario, ma trasmette le informazioni per accelerare il rilevamento dell'estremità remota dopo la modifica da `in avanti`.	Non trunking

	accetta la modifica.		

Ecco alcune caratteristiche salienti del protocollo:

- Il DTP presume una connessione point-to-point e i dispositivi Cisco supportano solo porte trunk 802.1Q point-to-point.
- Durante la negoziazione DTP, le porte non partecipano a STP. Solo quando la porta diventa uno dei tre tipi DTP (access, ISL o 802.1Q), la porta può essere aggiunta a STP. In caso contrario, PAgP, se configurato, è il processo successivo da eseguire prima che la porta partecipi a STP.
- Se la porta è trunking in modalità ISL, i pacchetti DTP vengono inviati sulla VLAN 1, altrimenti (per le porte trunking 802.1Q o non trunking) vengono inviati sulla VLAN nativa.
- In modalità `desiderabile`, i pacchetti DTP trasferiscono **il nome di dominio VTP** (che deve corrispondere per far comparire un trunk negoziato), oltre alla configurazione del trunk e **allo stato di amministrazione**.
- I messaggi vengono inviati ogni secondo durante la negoziazione e ogni 30 secondi dopo tale operazione.
- Accertarsi di aver compreso che le modalità `on`, `nonegotiate` e `off` specificano esplicitamente lo stato in cui la porta termina. Una configurazione errata può portare a uno stato pericoloso/incoerente in cui un lato è trunking e l'altro no.
- Una porta in modalità `on`, `auto`, o `desiderabile` invia periodicamente frame DTP. Se una porta in modalità `auto` o `desiderabile` non legge un pacchetto DTP in cinque minuti, viene impostata sulla modalità non trunk.

Per ulteriori informazioni sull'ISL, fare riferimento a Configurazione del trunking ISL sugli switch Catalyst serie 5500/5000 e 6500/6000. Per ulteriori informazioni sugli switch 802.1Q, fare riferimento al trunking tra gli switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con incapsulamento 802.1Q con software Cisco CatOS.

Suggerimento

Cisco consiglia una configurazione trunk esplicita di `valori desiderabili` su entrambe le estremità. In questa modalità, gli operatori di rete possono considerare attendibili i messaggi di stato syslog e della riga di comando che indicano che una porta è attiva e trunking, a differenza della modalità `on`, che consente di visualizzare una porta anche se il router adiacente non è configurato correttamente. Inoltre, il trunk in modalità `desiderabile` garantisce la stabilità in situazioni in cui un lato del collegamento non può diventare un trunk o cede lo stato del trunk. Per impostare la modalità `desiderata`, usare questo comando:

```
set trunk mod/port desirable ISL | dot1q
```

Nota: impostare il trunk su `off` su tutte le porte non trunk. In questo modo si eliminano gli sprechi di tempo di negoziazione quando si attivano le porte host. Questo comando viene eseguito anche quando si usa il comando **set port host**; per ulteriori informazioni, consultare la sezione STP. Per disabilitare un trunk su un intervallo di porte, eseguire questo comando:

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Altre opzioni

Un'altra configurazione comune del cliente utilizza la modalità `desiderabile` solo a livello di distribuzione e la configurazione predefinita più semplice (modalità `automatica`) a livello di accesso.

alcuni switch, ad esempio Catalyst 2900XL, router Cisco IOS o altri dispositivi del fornitore, non supportano al momento la negoziazione trunk tramite DTP. Sugli switch Catalyst 4500/4000, 5500/5000 e 6500/6000 è possibile utilizzare la modalità `non negoziazione` per impostare una porta in modo che il trunk con questi dispositivi venga eseguito in modo incondizionato, il che può contribuire a standardizzare un'impostazione comune in tutto il campus. Inoltre, è possibile implementare la modalità `non negoziazione` per ridurre il tempo "complessivo" di inizializzazione del collegamento.

Nota: fattori quali la modalità canale e la configurazione STP possono influire anche sul tempo di inizializzazione.

Per impostare la modalità `non negoziazione`, eseguire questo comando:

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco consiglia di `non negoziare` quando è presente una connessione a un router Cisco IOS perché, quando si esegue il bridging, alcuni frame DTP ricevuti dalla modalità **on** possono tornare alla porta trunk. Alla ricezione del frame DTP, la porta dello switch cerca di rinegoziare (o spostare il trunk verso il basso e verso l'alto) inutilmente. Se l'opzione `non negoziazione` è abilitata, lo switch non invia frame DTP.

Spanning Tree Protocol

Considerazioni di base

Il protocollo STP (Spanning Tree Protocol) mantiene un ambiente L2 privo di loop in reti commutate e bridge ridondanti. Senza STP, i frame loop e/o i multipli si moltiplicano in modo indefinito, il che provoca un collasso della rete. Tutti i dispositivi nel dominio di broadcast vengono interrotti continuamente da un traffico elevato.

Anche se per alcuni aspetti STP è un protocollo maturo inizialmente sviluppato per le specifiche bridge basate su software lento (IEEE 802.1d), può essere complesso implementarlo bene in reti a commutazione di grandi dimensioni con molte VLAN, molti switch in un dominio, supporto multi-vendor e nuovi miglioramenti IEEE.

Per riferimento futuro, CatOS 6.x continua ad adottare nuovi standard di sviluppo STP, quali il protocollo MISTP, il controllo dei loop, le root-guard e il rilevamento dell'inclinazione del tempo di arrivo BPDU. In CatOS 7.x sono inoltre disponibili ulteriori protocolli standardizzati, come lo Spanning Tree condiviso IEEE 802.1s e lo Spanning Tree di convergenza rapida IEEE 802.1w.

Panoramica operativa

La scelta del bridge radice per VLAN viene effettuata dallo switch con l'identificatore del bridge radice (BID) più basso. L'offerta è la priorità del bridge in combinazione con l'indirizzo MAC dello switch.

Inizialmente, le BPDU vengono inviate da tutti gli switch, contenenti l'offerta di ciascuno switch e il costo del percorso per raggiungere lo switch. In questo modo è possibile determinare il bridge radice e il percorso più economico alla radice. I parametri di configurazione aggiuntivi contenuti nelle BPDU della directory principale sostituiscono quelli configurati localmente in modo che l'intera rete utilizzi timer coerenti.

La topologia converge attraverso i seguenti passaggi:

1. Viene selezionato un singolo bridge radice per l'intero dominio Spanning Tree.
2. Una porta radice (rivolta verso il bridge radice) viene selezionata su ogni bridge non radice.
3. Viene selezionata una porta designata per l'inoltro BPDU su ciascun segmento.
4. Le porte non designate diventano bloccanti.

per ulteriori informazioni, fare riferimento a Configurazione dello Spanning Tree.

Impostazioni predefinite timer (secondi)	Nome	Funzione
2	Salve	Controlla l'invio di BPDU.
15	Ritardo Avanti (Fwddelay)	Controlla il tempo impiegato da una porta nello stato di ascolto e apprendimento e influenza il processo di modifica della topologia (vedere la sezione successiva).
20	Maxage	Controlla per quanto tempo lo switch conserva la topologia corrente prima di cercare un percorso alternativo. Dopo il numero massimo di secondi, una BPDU viene considerata obsoleta e lo switch cerca una nuova porta radice nel pool di porte bloccanti. Se non è disponibile alcuna porta bloccata, questa si definisce come la radice stessa sulle porte designate.

Stati porta	Significato	Intervallo predefinito allo stato successivo
Disattivato	Amministrativamente inattivo.	N/D
Blocco	Ricezione di BPDU e arresto dei dati utente.	Monitoraggio della ricezione di BPDU. Attendere 20 secondi per la scadenza massima o la modifica immediata se viene rilevato un errore del collegamento diretto/locale.

Ascolto	Invio o ricezione di BPDU per verificare se è necessario tornare al blocco.	Timer Fwddelay (attesa 15 secondi)
Apprendimento	Creazione della tabella di topologia/CAM.	Timer Fwddelay (attesa 15 secondi)
Inoltro	Invio/ricezione di dati.	
	Totale modifiche alla topologia di base:	**20 + 2 (15) = 50 secondi se si attende la scadenza di Maxage o 30 secondi se si verifica un errore di collegamento diretto**

I due tipi di BPDU in STP sono BPDU di configurazione e BPDU TCN (Topology Change Notification).

Flusso BPDU di configurazione

I BPDU di configurazione vengono inviati ogni volta che si verifica un intervallo di attesa da ciascuna porta sul bridge radice e successivamente vengono inviati a tutti gli switch foglia per mantenere lo stato dello Spanning Tree. In stato stazionario, il flusso BPDU è unidirezionale: le porte radice e le porte che bloccano ricevono solo BPDU di configurazione, mentre le porte designate inviano solo BPDU di configurazione.

Per ogni BPDU ricevuto da uno switch dalla directory principale, ne viene elaborato uno nuovo dal protocollo NMP centrale Catalyst e inviato contenente le informazioni sulla directory principale. In altre parole, se il bridge radice viene perso o tutti i percorsi al bridge radice vengono persi, la ricezione dei BPDU viene interrotta (fino a quando il timer massimo non inizia la rielezione).

Flusso BPDU TCN

I BPDU TCN vengono originati dagli switch foglia e fluiscono verso il bridge radice quando viene rilevata una modifica della topologia nello spanning tree. Le porte radice inviano solo i TCN e le porte designate ricevono solo i TCN.

Il BPDU TCN viaggia verso la cresta radice e viene riconosciuto ad ogni passaggio, quindi questo è un meccanismo affidabile. Una volta raggiunto il bridge radice, il bridge radice avvisa l'intero dominio che è stata apportata una modifica individuando le BPDU di configurazione con il flag TCN impostato sul tempo **`max + fwddelay`** (35 secondi per impostazione predefinita). In questo modo, tutti gli switch modificano il loro tempo di durata normale da cinque minuti (per impostazione predefinita) all'intervallo specificato da **`fwddelay`** (15 secondi per impostazione predefinita). per ulteriori informazioni, fare riferimento a Informazioni sulle modifiche della topologia dello Spanning Tree Protocol.

Modalità Spanning Tree

Per correlare le VLAN allo Spanning Tree, è possibile procedere in tre modi:

- uno Spanning Tree singolo per tutte le VLAN o un protocollo Spanning Tree mono, ad esempio IEEE 802.1Q
- uno Spanning Tree per VLAN o uno Spanning Tree condiviso, ad esempio Cisco PVST
- uno Spanning Tree per set di VLAN o più Spanning Tree, come Cisco MISTP e IEEE 802.1s

Uno Spanning Tree mono per tutte le VLAN consente solo una topologia attiva e quindi nessun bilanciamento del carico. Un STP ha bloccato le porte di tutte le VLAN e non trasporta dati.

Uno Spanning Tree per VLAN consente il bilanciamento del carico, ma richiede una maggiore elaborazione della CPU BPDU all'aumentare del numero di VLAN. Le note di rilascio di CatOS forniscono indicazioni sul numero di porte logiche consigliate nello Spanning Tree per switch. Ad esempio, la formula di Catalyst 6500/6000 Supervisor Engine 1 è la seguente:

numero di porte + (numero di trunk * numero di VLAN sui trunk) < 4000

Cisco MISTP e il nuovo standard 802.1s consentono di definire solo due istanze/topologie STP attive e di mappare tutte le VLAN su uno di questi due alberi. Questa tecnica consente la scalabilità di STP a molte migliaia di VLAN mentre è abilitato il bilanciamento del carico.

Formati BPDU

Per supportare lo standard IEEE 802.1Q, l'implementazione Cisco STP esistente è stata estesa fino a diventare PVST+ aggiungendo il supporto per il tunneling in una regione dello Spanning Tree monocromatica IEEE 802.1Q. PVST+ è pertanto compatibile sia con i protocolli MST IEEE 802.1Q che con i protocolli PVST Cisco e non richiede comandi o configurazioni aggiuntivi. Inoltre, PVST+ aggiunge meccanismi di verifica per garantire che non vi siano incoerenze di configurazione tra il trunking della porta e gli ID VLAN sugli switch.

Di seguito sono riportate alcune caratteristiche operative del protocollo PVST+:

- PVST+ interagisce con lo Spanning Tree monocromatico 802.1Q attraverso il cosiddetto CST (Common Spanning Tree) su un trunk 802.1Q. Poiché il CST si trova sempre sulla VLAN 1, questa VLAN deve essere abilitata sul trunk per interagire con gli altri fornitori. Le BPDU CST vengono trasmesse, sempre senza tag, al Bridge-Group standard IEEE (indirizzo MAC 01-80-c2-00-00-00, DSAP 42, SSAP 42). Per una descrizione completa, un gruppo parallelo di BPDU viene trasmesso anche all'indirizzo MAC dello Spanning Tree condiviso di Cisco per la VLAN 1.
- PVST+ crea tunnel PVST BPDU su regioni VLAN 802.1Q come dati multicast. Le BPDU Cisco shared Spanning Tree vengono trasmesse all'indirizzo MAC 01-00-0c-cc-cc-cd (tipo di protocollo SNAP HDLC 0x010b) per ciascuna VLAN su un trunk. Le BPDU non hanno tag sulla VLAN nativa e sono tag su tutte le altre VLAN.
- PVST+ verifica le incoerenze tra le porte e le VLAN. PVST+ blocca le porte che ricevono BPDU incoerenti per impedire i loop di inoltro. Tramite messaggi syslog, notifica inoltre agli utenti eventuali configurazioni non corrispondenti.
- PVST+ è compatibile con gli switch Cisco esistenti che eseguono PVST su trunk ISL. I BPDU incapsulati dall'ISL vengono ancora trasmessi o ricevuti utilizzando l'indirizzo MAC IEEE. In altre parole, ogni tipo BPDU è locale al collegamento; non ci sono problemi di traduzione.

Suggerimento

Per impostazione predefinita, su tutti gli switch Catalyst il protocollo STP è abilitato. Questa opzione è consigliata anche se si sceglie un progetto che non include loop L2 in modo che STP non sia abilitato nel senso che sta mantenendo attivamente una porta bloccata.

```
set spantree enable all
!--- This is the default.
```

Cisco consiglia di lasciare abilitato STP per i seguenti motivi:

- Se si verifica un loop (causato da patch non corrette, cavo errato e così via), il protocollo STP impedisce gli effetti negativi sulla rete causati da dati multicast e broadcast.
- Protezione contro il guasto di EtherChannel.
- La maggior parte delle reti è configurata con STP, che le consente la massima esposizione sul campo. Una maggiore esposizione in genere equivale a un codice stabile.
- Protezione contro il funzionamento errato di due schede NIC collegate (o il bridging abilitato sui server).
- Il software per molti protocolli (come PAgP, snooping IGMP e trunking) è strettamente correlato a STP. L'esecuzione senza STP può produrre risultati indesiderati.

Non modificare i timer, in quanto ciò potrebbe influire negativamente sulla stabilità. La maggior parte delle reti installate non viene sintonizzata. I semplici timer STP accessibili tramite la riga di comando, come hello-interval e Maxage, sono a loro volta costituiti da un insieme complesso di altri timer presunti e intrinseci, quindi è difficile regolare i timer e considerare tutte le ramificazioni. Esiste inoltre il pericolo di compromettere la protezione UDLD.

In teoria, è opportuno tenere il traffico degli utenti lontano dalla VLAN di gestione. Specialmente con i vecchi processori degli switch Catalyst, è meglio evitare problemi con STP mantenendo la VLAN di gestione separata dai dati dell'utente. Una stazione terminale che si comporta in modo errato potrebbe potenzialmente tenere il processore del supervisor engine così occupato con i pacchetti di broadcast da perdere una o più BPDU. Tuttavia, gli switch più recenti con CPU più potenti e controlli di limitazione attenuano questa considerazione. Per ulteriori informazioni, vedere la sezione Gestione in banda di questo documento.

Non sovraprogettare la ridondanza. Ciò può causare un incubo di risoluzione dei problemi: troppe porte bloccate influiscono negativamente sulla stabilità a lungo termine. **Mantenere il diametro totale del TSS al di sotto di sette luppoli**. Provare a progettare secondo il modello multilayer di Cisco, con i suoi domini a commutazione ridotta, i triangoli STP e le porte bloccate deterministiche (come spiegato in Gigabit Campus Network Design—Principles and Architecture) quando possibile.

Consente di determinare e conoscere la posizione delle funzionalità principali e delle porte bloccate e di documentarle nel diagramma della topologia. Le porte bloccate sono il punto in cui inizia la risoluzione dei problemi STP - ciò che le ha fatte passare dal blocco all'inoltro è spesso la parte chiave dell'analisi della causa principale. **Scegliere i livelli di distribuzione e core come posizione della radice principale/secondaria**, poiché sono considerati le parti più stabili della rete. Verificare la sovrapposizione L3 e HSRP ottimale con i percorsi di inoltro dati L2. Questo comando è una macro che configura la priorità del bridge; root lo imposta su un valore di gran lunga inferiore rispetto al valore predefinito (32768), mentre il valore di root secondario lo imposta su un valore ragionevolmente inferiore rispetto al valore predefinito:

```
set spantree root secondary vlan range
```

Nota: questa macro imposta la priorità radice su 8192 (per impostazione predefinita), la priorità radice corrente meno 1 (se è noto un altro bridge radice) o la priorità radice corrente (se l'indirizzo MAC è inferiore alla radice corrente).

Eliminare le VLAN non necessarie dalle porte trunk (un esercizio bidirezionale). Ciò limita il diametro del sovraccarico di elaborazione di STP e NMP su parti della rete in cui alcune VLAN non sono necessarie. L'eliminazione automatica VTP non rimuove il protocollo STP da un trunk. Fare riferimento alla sezione VTP di questo documento per ulteriori informazioni. La VLAN predefinita 1 può anche essere rimossa dai trunk usando CatOS 5.4 e versioni successive.

per ulteriori informazioni, fare riferimento a Problemi del protocollo Spanning Tree e considerazioni di progettazione correlate.

Altre opzioni

Cisco offre un altro STP noto **come VLAN-bridge**. Questo protocollo funziona usando un indirizzo MAC di destinazione di **01-00-0c-cd-cd-ce** e un tipo di protocollo di 0x010c.

Questa funzione è particolarmente utile quando è necessario eseguire il bridge di protocolli non instradabili o legacy tra VLAN senza interferire con le istanze dello Spanning Tree IEEE in esecuzione su tali VLAN. Se le interfacce VLAN per il traffico non bridge vengono bloccate per il traffico L2 (e questo potrebbe accadere facilmente se partecipassero allo stesso STP delle VLAN IP), anche il traffico L3 in sovrapposizione viene potato inavvertitamente - un effetto collaterale indesiderato. Il bridge VLAN è pertanto un'istanza separata di STP per i protocolli con bridging, che fornisce una topologia separata che può essere manipolata senza influire sul traffico IP.

Se è necessario un bridging tra VLAN su router Cisco come l'MSFC, si consiglia di eseguire il bridging tra VLAN.

PortFast

PortFast viene utilizzata per ignorare il normale funzionamento dello Spanning Tree sulle porte di accesso e per velocizzare la connettività tra le unità terminali e i servizi a cui devono connettersi dopo l'inizializzazione del collegamento. Su alcuni protocolli, come IPX/SPX, è importante vedere la porta di accesso in modalità di inoltro subito dopo che lo stato del collegamento è diventato attivo per evitare problemi GNS.

per ulteriori informazioni, fare riferimento a Utilizzo di Portfast e di altri comandi per correggere i ritardi della connettività di avvio della workstation.

Panoramica operativa

PortFast ignora i normali stati di `ascolto` e `apprendimento` di STP spostando una porta direttamente dalla modalità di `blocco` alla modalità di `inoltro` dopo che il collegamento è notoriamente in esecuzione. Se questa funzione non è abilitata, STP elimina tutti i dati utente finché non decide che la porta è pronta per essere spostata nella modalità di `inoltro`. Questa operazione può richiedere fino al doppio del tempo di `ForwardDelay` (per impostazione predefinita, un totale di 30 secondi).

La modalità PortFast impedisce inoltre che venga generato un TCN STP ogni volta che lo stato di una porta cambia da `apprendimento` a `inoltro`. I cittadini di paesi terzi non sono un problema di per sé, ma se un'ondata di cittadini di paesi terzi colpisce il ponte principale (in genere la mattina quando le persone accendono i loro PC), potrebbe prolungare inutilmente il tempo di convergenza.

STP PortFast è particolarmente importante nelle reti multicast CGMP e Catalyst 5500/5000 MLS. In questi ambienti, i TCN possono causare il timeout delle voci statiche della tabella CGMP CAM, con conseguente perdita di pacchetti multicast fino al successivo report IGMP, e/o lo scaricamento delle voci della cache MLS che devono essere ricostruite e possono causare un picco della CPU del router, a seconda delle dimensioni della cache. (le implementazioni MLS e le voci multicast di Catalyst 6500/6000 apprese dallo snooping IGMP non sono interessate).

Suggerimento

Cisco consiglia di abilitare STP PortFast per tutte le porte host attive e di disabilitarlo per i collegamenti degli switch e le porte non in uso.

Anche il trunking e il channeling devono essere disabilitati per tutte le porte host. Per impostazione predefinita, ciascuna porta di accesso è abilitata per il trunking e il channeling, ma sulle porte host le porte adiacenti allo switch non sono progettate appositamente. Se questi protocolli vengono lasciati alla negoziazione, il successivo ritardo nell'attivazione della porta può causare situazioni indesiderate in cui i pacchetti iniziali provenienti dalle workstation, ad esempio le richieste DHCP, non vengono inoltrati.

CatOS 5.2 ha introdotto un comando macro, **set port host *port range***, che implementa questa configurazione delle porte di accesso e aiuta in modo significativo la negoziazione automatica e le prestazioni della connessione:

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

Nota: PortFast non significa che lo Spanning Tree non venga eseguito su queste porte. Le BPDU vengono ancora inviate, ricevute ed elaborate.

Altre opzioni

PortFast BPDU-guard consente di prevenire i loop spostando una porta non trunking in stato `err-disabled` quando si riceve una BPDU su tale porta.

Un pacchetto BPDU non deve mai essere ricevuto su una porta di accesso configurata per PortFast, in quanto le porte host non devono essere collegate agli switch. Se viene rilevata una BPDU, indica una configurazione non valida e probabilmente pericolosa che richiede un intervento amministrativo. Quando la funzione BPDU-guard è abilitata, lo Spanning Tree chiude le interfacce configurate con PortFast che ricevono BPDU anziché metterle nello stato di `blocco` STP.

Il comando funziona per switch, non per porta, come mostrato:

```
set spantree portfast bpdu-guard enable
```

Al gestore della rete viene inviata una notifica tramite trap SNMP o messaggio syslog se la porta non funziona. Inoltre, è possibile configurare un tempo di ripristino automatico per le porte disabilitate a causa di un errore. Fare riferimento alla sezione UDLD di questo documento per ulteriori dettagli. Per ulteriori informazioni, consultare il documento sui miglioramenti della funzionalità Spanning Tree Portfast BPDU Guard.

Nota: PortFast per le porte trunk è stato introdotto in CatOS 7.x e non ha alcun effetto sulle porte trunk nelle versioni precedenti. PortFast per porte trunk è progettato per aumentare i tempi di convergenza per le reti L3. Per integrare questa funzione, CatOS 7.x ha introdotto anche la possibilità di configurare PortFast BPDU-guard su base per porta.

UplinkFast

UplinkFast fornisce una rapida convergenza STP dopo un errore di collegamento diretto nel livello di accesso alla rete. Non modifica l'STP, e il suo scopo è quello di accelerare il tempo di convergenza in una specifica circostanza a meno di tre secondi, invece del tipico ritardo di 30 secondi. per ulteriori informazioni, fare riferimento a Descrizione e configurazione della funzione Cisco Uplink Fast.

Panoramica operativa

Utilizzando il modello di progettazione multilivello Cisco sul livello di accesso, se l'uplink di inoltro viene perso, l'uplink di blocco viene immediatamente spostato su uno stato di `inoltro` senza attendere gli stati di `ascolto` e di `apprendimento`.

Un gruppo uplink è un set di porte per VLAN che possono essere considerate come una porta radice e una porta radice di backup. In condizioni normali, le porte radice assicurano la connettività dall'accesso verso la radice. Se per qualsiasi motivo la connessione principale alla radice si interrompe, il collegamento alla radice di backup viene attivato immediatamente senza che sia necessario attendere circa 30 secondi prima che la convergenza avvenga.

Poiché in questo modo viene ignorato il normale processo di gestione delle modifiche della topologia STP (`ascolto` e `apprendimento`), è necessario un meccanismo alternativo di correzione della topologia per aggiornare gli switch nel dominio in modo che le stazioni terminali locali siano raggiungibili tramite un percorso alternativo. Lo switch del livello di accesso con UplinkFast genera inoltre frame per ciascun indirizzo MAC nella propria CAM a un indirizzo MAC multicast (01-00-0c-cd-cd-cd, protocollo HDLC 0x200a) per aggiornare la tabella CAM in tutti gli switch del dominio con la nuova topologia.

Suggerimento

Cisco consiglia di abilitare UplinkFast per gli switch con porte bloccate, in genere al livello di accesso. Non utilizzare sugli switch senza la conoscenza della topologia implicita di un root link di backup, in genere switch di distribuzione e core in un design multilayer di Cisco. Può essere aggiunto senza interruzioni alla rete di produzione. Per abilitare UplinkFast, usare questo comando:

```
set spantree uplinkfast enable
```

Questo comando imposta anche la **priorità** del **bridge** su alta per ridurre al minimo il rischio che diventi un bridge radice e la **priorità** della **porta su** alta per ridurre al minimo il rischio che diventi una porta designata, compromettendo così la funzionalità. Quando si ripristina uno switch con UplinkFast abilitata, la funzione deve essere disabilitata, il database uplink viene cancellato con "clear uplink" e le priorità del bridge vengono ripristinate manualmente.

Nota: la parola chiave **all protocols** per il comando UplinkFast è necessaria quando è abilitata la funzione di filtro dei protocolli. Poiché il CAM registra il tipo di protocollo e le informazioni MAC e VLAN quando il filtro del protocollo è abilitato, è necessario generare un frame UplinkFast per ciascun protocollo su ciascun indirizzo MAC. La parola chiave **rate** indica i pacchetti al secondo dei frame di aggiornamento della topologia uplinkfast. L'impostazione predefinita è consigliata. Non è necessario configurare BackboneFast con Rapid STP (RSTP) o IEEE 802.1w perché il meccanismo è incluso in modo nativo e abilitato automaticamente in RSTP.

BackboneFast

BackboneFast fornisce una rapida convergenza da errori di collegamento indiretti. Grazie alle nuove funzionalità di STP, i tempi di convergenza possono essere ridotti da 50 a 30 secondi.

Panoramica operativa

Il meccanismo viene avviato quando una porta radice o una porta bloccata su uno switch riceve BPDU inferiori dal bridge designato. Questo problema può verificarsi quando uno switch a valle perde la connessione con la radice e inizia a inviare le proprie BPDU per selezionare una nuova radice. Una **BPDU inferiore** identifica uno switch sia come bridge radice sia come bridge designato.

In base alle normali regole dello Spanning Tree, lo switch ricevente ignora i BPDU inferiori per il tempo di aging massimo configurato, 20 secondi per impostazione predefinita. Tuttavia, con BackboneFast, lo switch vede la BPDU inferiore come un segnale che la topologia potrebbe essere stata modificata e cerca di determinare se dispone di un percorso alternativo al bridge radice tramite BPDU Root Link Query (RLQ). Questa aggiunta di protocollo consente a uno switch di controllare se la radice è ancora disponibile, sposta una porta `bloccata` all'`inoltro` in meno tempo e notifica allo switch isolato che ha inviato la BPDU inferiore che la radice è ancora presente.

Di seguito sono riportati alcuni punti salienti del funzionamento del protocollo:

- Uno switch trasmette il pacchetto RLQ solo dalla porta radice (verso il bridge radice).
- Uno switch che riceve un RLQ può rispondere se è lo switch radice o se sa di aver perso la connessione con la radice. Se non è a conoscenza di questi fatti, deve inoltrare la query alla porta principale.
- Se un'opzione ha perso la connessione alla directory principale, deve rispondere in negativo a questa query.
- La risposta deve essere inviata solo dalla porta da cui proviene la query.
- Il parametro radice deve sempre rispondere alla query con una risposta positiva.
- Se la risposta viene ricevuta su una porta non radice, viene scartata.

I tempi di convergenza STP possono essere ridotti fino a 20 secondi, in quanto maxage non ha bisogno di scadere.

per ulteriori informazioni, fare riferimento a Comprensione e configurazione della backbone Fast sugli switch Catalyst.

Suggerimento

Si consiglia di abilitare BackboneFast su tutti gli switch con STP. Può essere aggiunto senza interruzioni alla rete di produzione. Per abilitare BackboneFast, usare questo comando:

```
set spantree backbonefast enable
```

Nota: questo comando a livello globale deve essere configurato su tutti gli switch di un dominio perché aggiunge al protocollo STP una funzionalità che tutti gli switch devono comprendere.

Altre opzioni

BackboneFast non è supportato sugli switch serie 2900XL e 3500. Non deve essere abilitato se il dominio dello switch contiene questi switch oltre agli switch Catalyst 4500/4000, 5500/5000 e 6500/6000.

Non è necessario configurare BackboneFast con RSTP o IEEE 802.1w perché il meccanismo è incluso in modo nativo e abilitato automaticamente in RSTP.

Spanning Tree Loop Guard

Loop Guard è un'ottimizzazione proprietaria di Cisco per STP. Protezione loop protegge le reti L2 dai loop causati da:

- Interfacce di rete che non funzionano correttamente
- CPU occupate
- Qualsiasi cosa che impedisca l'inoltro normale delle BPDU

Un loop STP si verifica quando una porta di blocco in una topologia ridondante passa erroneamente allo stato di inoltro. Questa transizione in genere si verifica perché una delle porte in una topologia fisicamente ridondante (non necessariamente la porta di blocco) cessa di ricevere BPDU.

La funzione Loop Guard è utile solo nelle reti commutate in cui gli switch sono connessi tramite collegamenti point-to-point. La maggior parte delle moderne reti di campus e centri dati sono di questo tipo. In un collegamento point-to-point, un bridge designato non può scomparire a meno che non invii una BPDU inferiore o non riduca il collegamento. La funzione STP loop guard è stata introdotta in CatOS versione 6.2(1) per le piattaforme Catalyst 4000 e Catalyst 5000 e nella versione 6.2(2) per la piattaforma Catalyst 6000.

per ulteriori informazioni sul controllo loop, fare riferimento a Miglioramenti del protocollo Spanning-Tree con le funzionalità Loop Guard e BPDU Skew Detection.

Panoramica operativa

Loop Guard verifica se una porta radice o una porta radice alternativa/di backup riceve BPDU. Se

la porta non riceve BPDU, la protezione del loop mette la porta in uno stato incoerente (blocco) finché la porta non ricomincia a ricevere BPDU. Una porta in stato incoerente non trasmette pacchetti BPDU. Se una porta di questo tipo riceve nuovamente i BPDU, la porta (e il collegamento) vengono considerati nuovamente validi. La condizione di loop incoerente viene rimossa dalla porta e il protocollo STP determina lo stato della porta in quanto tale ripristino è automatico.

La protezione loop isola l'errore e consente allo spanning tree di convergere in una topologia stabile senza il collegamento o il bridge in errore. Protezione loop impedisce i loop STP con la velocità della versione STP in uso. Non vi è alcuna dipendenza da STP stesso (802.1d o 802.1w) o quando i timer STP sono sintonizzati. Per questi motivi, implementare la protezione loop insieme a UDLD nelle topologie che si basano su STP e in cui il software supporta le funzionalità.

Quando il controllo loop blocca una porta incoerente, viene registrato questo messaggio:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

Quando la BPDU viene ricevuta su una porta in uno stato STP con loop incoerente, la porta passa a un altro stato STP. In base alla BPDU ricevuta, il ripristino è automatico e non è necessario alcun intervento. Dopo il ripristino, il messaggio viene registrato.

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

Interazione con altre funzioni STP

- **Protezione radice**La funzione Root Guard forza la designazione di una porta sempre. Loop Guard è effettivo solo se la porta è la porta radice o una porta alternativa. Queste funzioni si escludono a vicenda. Non è possibile abilitare contemporaneamente Loop Guard e Root Guard su una porta.
- **UplinkFast**Loop Guard è compatibile con UplinkFast. Se la protezione loop imposta una porta radice in uno stato di blocco, UplinkFast imposta una nuova porta radice nello stato di inoltro. Inoltre, UplinkFast non seleziona una porta con loop incoerente come porta radice.
- **BackboneFast**Loop Guard è compatibile con BackboneFast. La ricezione di una BPDU inferiore proveniente da un bridge designato attiva BackboneFast. Poiché i BPDU vengono ricevuti da questo collegamento, la protezione loop non è attivata, quindi BackboneFast e la protezione loop sono compatibili.
- **PortFast**PortFast esegue il passaggio di una porta allo stato designato per l'inoltro subito dopo il collegamento. Poiché una porta abilitata per PortFast non può essere una porta radice o alternativa, la protezione loop e PortFast si escludono a vicenda.
- **PAgP**Loop Guard utilizza le porte conosciute per STP. Pertanto, la protezione loop può sfruttare l'astrazione delle porte logiche fornite da PAgP. Tuttavia, per formare un canale, tutte le porte fisiche raggruppate nel canale devono avere configurazioni compatibili. PAgP applica la configurazione uniforme della protezione loop su tutte le porte fisiche per formare un canale.**Nota:** quando si configura la protezione loop su EtherChannel, vengono visualizzati i seguenti avvertimenti:STP sceglie sempre la prima porta operativa del canale per inviare i BPDU. Se il collegamento diventa unidirezionale, la protezione del loop blocca il canale, anche se altri collegamenti nel canale funzionano correttamente.Se le porte che sono già bloccate da una protezione in loop vengono raggruppate per formare un canale, STP perde tutte le informazioni sullo stato di tali porte. La nuova porta del canale può raggiungere lo

stato di inoltro con un ruolo designato.Se un canale è bloccato da una protezione in loop e il canale si interrompe, STP perde tutte le informazioni sullo stato. Le singole porte fisiche possono raggiungere lo stato di inoltro con il ruolo designato, anche se uno o più collegamenti che hanno formato il canale sono unidirezionali.Negli ultimi due casi dell'elenco, è possibile che si verifichi un loop finché il protocollo UDLD non rileva il problema. Ma la protezione loop non è in grado di rilevare il loop.

Confronto tra le funzionalità di Loop Guard e UDLD

La funzionalità di protezione del ciclo e la funzionalità UDLD si sovrappongono parzialmente. Entrambi proteggono dagli errori STP causati dai collegamenti unidirezionali. Ma queste due caratteristiche sono diverse nell'approccio al problema e anche nella funzionalità. In particolare, esistono alcuni errori unidirezionali che UDLD non è in grado di rilevare, ad esempio errori causati da una CPU che non invia pacchetti BPDU. Inoltre, l'uso di timer STP aggressivi e della modalità RSTP può generare loop prima che il protocollo UDLD possa rilevare gli errori.

Loop Guard non funziona sui collegamenti condivisi o nelle situazioni in cui il collegamento è stato unidirezionale dopo il collegamento. Nel caso in cui il collegamento sia stato unidirezionale dopo il collegamento, la porta non riceve mai pacchetti BPDU e viene designata. Questo comportamento può essere normale, quindi la protezione loop non copre questo caso particolare. UDLD offre protezione contro uno scenario di questo tipo.

Abilitare sia UDLD che loop guard per fornire il più alto livello di protezione. Per un confronto tra le funzionalità loop Guard e UDLD, consultare la sezione *Confronto tra le funzionalità Loop Guard e Unidirectional Link Detection* dei miglioramenti dello Spanning-Tree Protocol che usano le funzionalità Loop Guard e BPDU Skew Detection.

Suggerimento

Cisco consiglia di abilitare la protezione loop a livello globale su una rete di switch con loop fisici. Nella versione 7.1(1) del software Catalyst e successive, è possibile abilitare la protezione loop a livello globale su tutte le porte. La funzione è effettivamente attivata su tutti i collegamenti point-to-point. Lo stato duplex del collegamento rileva il collegamento point-to-point. Se il duplex è pieno, il collegamento viene considerato point-to-point. Per abilitare la protezione del loop globale, eseguire questo comando:

```
set spantree global-default loopguard enable
```

Altre opzioni

Per gli switch che non supportano la configurazione globale loop guard, abilitare la funzione su tutte le singole porte, incluse le porte del canale della porta. Sebbene non vi siano vantaggi nell'abilitazione della protezione loop su una porta designata, questa abilitazione non è un problema. Inoltre, una riconvergenza valida dello Spanning Tree può trasformare una porta designata in una porta radice, rendendo la funzione utile su questa porta. Per abilitare la protezione loop, usare questo comando:

```
set spantree guard loop mod/port
```

Le reti con topologie prive di loop possono comunque beneficiare della protezione in loop nel caso in cui i loop vengano introdotti accidentalmente. Tuttavia, l'abilitazione della protezione loop in questo tipo di topologia può causare problemi di isolamento rete. Per creare topologie senza loop ed evitare problemi di isolamento della rete, eseguire questi comandi per disabilitare la protezione loop a livello globale o singolarmente. Non abilitare la protezione del loop sui collegamenti condivisi.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```

  o
- ```
  set spantree guard none mod/port
  !--- This is the default port configuration.
  ```

Spanning Tree Root Guard

La funzionalità Root Guard offre un modo per applicare la posizione del root bridge nella rete. Root Guard assicura che la porta su cui root guard è abilitato sia la porta designata. In genere, tutte le porte del root bridge sono porte designate, a meno che due o più porte del root bridge non siano collegate tra loro. Se il bridge riceve pacchetti BPDU STP superiori su una porta abilitata per la protezione radice, sposta questa porta in uno stato STP non coerente per la radice. Lo stato di incoerenza root è l'equivalente dello stato di ascolto. Su questa porta il traffico non viene reindirizzato, In questo modo, la root guard applica la posizione del root bridge. Root Guard è disponibile in CatOS per Catalyst 29xx, 4500/4000, 5500/5000 e 6500/6000 nella versione software 6.1.1 e successive.

Panoramica operativa

Root Guard è un meccanismo incorporato di STP. Root Guard non dispone di un proprio timer e si basa solo sulla ricezione di BPDU. Quando root guard viene applicato a una porta, non consente che una porta diventi una porta radice. Se la ricezione di una BPDU attiva una convergenza dello Spanning Tree che rende una porta designata una porta radice, la porta viene messa in uno stato incoerente per la radice. Il messaggio syslog mostra l'azione:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

Quando la porta non invia più BPDU superiori, viene nuovamente sbloccata. Tramite STP, la porta passa dallo stato di ascolto allo stato di apprendimento e infine passa allo stato di inoltro. Il recupero è automatico e non è necessario alcun intervento umano. Questo messaggio syslog fornisce un esempio:

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

Root Guard forza la designazione di una porta e loop guard è efficace solo se la porta è la porta radice o una porta alternativa. Pertanto, le due funzioni si escludono a vicenda. Non è possibile abilitare contemporaneamente Loop Guard e Root Guard su una porta.

per ulteriori informazioni, fare riferimento al miglioramento della root guard dello Spanning Tree Protocol.

Suggerimento

Cisco consiglia di abilitare la funzione root guard sulle porte che si connettono a dispositivi di rete non sottoposti a controllo amministrativo diretto. Per configurare root guard, usare questo comando:

```
set spantree guard root mod/port
```

EtherChannel

Le tecnologie EtherChannel consentono il multiplexing inverso di più canali (fino a otto su Catalyst 6500/6000) in un unico collegamento logico. Sebbene ogni piattaforma differisca da quella successiva nell'implementazione, è importante comprendere i requisiti comuni:

- Algoritmo per il multiplex statistico di frame su più canali
- Creazione di una porta logica per l'esecuzione di una singola istanza di STP
- Protocollo di gestione dei canali, ad esempio PAgP o LACP (Link Aggregation Control Protocol)

Frame Multiplexing

EtherChannel comprende un algoritmo di distribuzione dei frame che esegue un multiplexing efficiente dei frame nei collegamenti 10/100 o Gigabit del componente. Le differenze negli algoritmi per piattaforma derivano dalla capacità di ciascun tipo di hardware di estrarre informazioni di frame header per prendere la decisione di distribuzione.

L'algoritmo di distribuzione del carico è un'opzione globale per entrambi i protocolli di controllo del canale. PAgP e LACP utilizzano l'algoritmo di distribuzione del frame perché lo standard IEEE non impone alcun algoritmo di distribuzione particolare. Tuttavia, qualsiasi algoritmo di distribuzione garantisce che, quando vengono ricevuti i frame, l'algoritmo non causi un ordinamento errato dei frame che fanno parte di una determinata conversazione o duplicazione di frame.

Nota: queste informazioni devono essere considerate:

- Catalyst 6500/6000 ha un hardware di switching più recente rispetto a Catalyst 5500/5000 e può leggere le informazioni IP Layer 4 (L4) alla velocità del cavo per prendere una decisione di multiplexing più intelligente delle semplici informazioni MAC L2.
- Le funzionalità di Catalyst 5500/5000 dipendono dalla presenza di un EBC (Ethernet Bundling Chip) sul modulo. Il comando **show port capabilities *mod/porta*** conferma le funzionalità disponibili per ciascuna porta.

Fare riferimento a questa tabella, che illustra in dettaglio l'algoritmo di distribuzione dei frame per ciascuna piattaforma elencata:

Piattaforma	Algoritmo di bilanciamento del carico del canale

ma	
Catalyst serie 5500/5000	Se il Catalyst 5500/5000 ha i moduli necessari, possono essere presenti da due a quattro collegamenti per FEC[1], anche se devono trovarsi sullo stesso modulo. Le coppie di indirizzi MAC di origine e destinazione determinano il collegamento scelto per l'inoltro dei frame. Un'operazione X-OR viene eseguita sui due bit meno significativi dell'indirizzo MAC di origine e dell'indirizzo MAC di destinazione. Questa operazione consente di ottenere uno dei quattro risultati seguenti: (0 0), (0 1), (1 0) o (1 1). Ognuno di questi valori indica un collegamento nel bundle FEC. Nel caso di un Fast EtherChannel a due porte, solo un bit singolo viene utilizzato nell'operazione X-OR. Possono verificarsi circostanze in cui un indirizzo nella coppia origine/destinazione è una costante. Ad esempio, la destinazione può essere un server o, più probabilmente, un router. In questo caso, viene visualizzato il bilanciamento del carico statistico perché l'indirizzo di origine è sempre diverso.
Catalyst serie 4500/4000	Catalyst 4500/4000 EtherChannel distribuisce i frame sui collegamenti in un canale (su un singolo modulo) in base ai bit meno significativi degli indirizzi MAC di origine e destinazione di ciascun frame. Rispetto agli switch Catalyst 5500/5000, l'algoritmo è più coinvolto e usa un hash deterministico di questi campi di MAC DA (byte 3, 5, 6), SA (byte 3, 5, 6), porta in entrata e ID VLAN. Il metodo di distribuzione dei frame non è configurabile.
Catalyst serie 6500/6000	Esistono due possibili algoritmi di hash, a seconda dell'hardware del Supervisor Engine. L'hash è un polinomio a diciassette gradi implementato nell'hardware che, in tutti i casi, prende l'indirizzo MAC, l'indirizzo IP o il numero di porta IP TCP/UDP[2] e applica l'algoritmo per generare un valore a tre bit. Questa operazione viene eseguita separatamente per gli indirizzi di origine e di destinazione. I risultati vengono quindi XORd per generare un altro valore a tre bit che viene utilizzato per determinare la porta del canale da utilizzare per inoltrare il pacchetto. I canali sullo switch Catalyst 6500/6000 possono essere formati tra le porte di qualsiasi modulo e possono essere fino a 8 porte.

[1] FEC = Fast EtherChannel

[2] UDP = User Datagram Protocol

Questa tabella indica i metodi di distribuzione supportati sui vari modelli Catalyst 6500/6000 Supervisor Engine e il loro comportamento predefinito.

Hardware	Descrizione	Metodi di distribuzione
WS-F6020 (motore L2)	Early Supervisor Engine 1	MAC L2: SA DA SA e DA
WS-F6020A (motore L2) WS-F6K-PFC (motore L3)	In seguito Supervisor Engine 1 e Supervisor Engine 1A/PFC1	MAC L2: SA DA SA e DA L3 IP: SA DA SA e DA (impostazione predefinita)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (richiede CatOS 6.x)	MAC L2: SA DA SA e DA L3 IP: SA DA Sessione L4 SA & DA (predefinita): porta S; porto D; Porta S & D (predefinita)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3A (richiede CatOS 8.1.x) Supervisor Engine 720/Supervisor Engine 32/PFC3B (richiede CatOS 8.4.x) Supervisor Engine 720/PFC3BXL (richiede CatOS 8.3.x)	MAC L2: SA DA SA e DA L3 IP: SA DA Sessione L4 SA & DA (predefinita): porta S; porto D; Porta S & D IP-VLAN-L4 sessione: Porta SA & VLAN & S; Porta DA & VLAN & D; Porta SA & DA & VLAN & S e porta D

Nota: nella distribuzione L4, il primo pacchetto frammentato usa la distribuzione L4. Tutti i pacchetti successivi usano la distribuzione L3.

Per ulteriori informazioni sul supporto di EtherChannel su altre piattaforme e su come configurarle e risolverle, consultare i seguenti documenti:

- Informazioni sul bilanciamento del carico EtherChannel e sulla ridondanza negli switch Catalyst
- Configurazione di EtherChannel tra gli switch Catalyst 4500/4000, 5500/5000 e 6500/6000 con CatOS System Software
- Configurazione di LACP (802.3ad) tra un Catalyst 6500/6000 e un Catalyst 4500/4000
- Configurazione di EtherChannel layer 3 e layer 2

Suggerimento

Per impostazione predefinita, gli switch Catalyst serie 6500/6000 eseguono il bilanciamento del carico in base all'indirizzo IP. Questa impostazione è consigliata in CatOS 5.5, presupponendo che IP sia il protocollo dominante. Per impostare il bilanciamento del carico, usare questo comando:

```
set port channel all distribution ip both
!--- This is the default.
```

La distribuzione dei frame Catalyst serie 4500/4000 e 5500/5000 tramite indirizzo MAC L2 è accettabile nella maggior parte delle reti. Tuttavia, lo stesso collegamento viene utilizzato per tutto il traffico se vi sono solo due dispositivi principali che comunicano su un canale (poiché SMAC e DMAC sono costanti). Questo problema può in genere verificarsi per il backup del server e altri trasferimenti di file di grandi dimensioni o per un segmento di transito tra due router.

Anche se la porta di aggregazione logica (agport) può essere gestita dal protocollo SNMP come istanza separata e le statistiche aggregate sul throughput raccolte, Cisco consiglia comunque di gestire ciascuna delle interfacce fisiche separatamente per verificare il funzionamento dei meccanismi di distribuzione dei frame e se viene raggiunto il bilanciamento del carico statistico.

Un nuovo comando, il comando show channel traffic , in CatOS 6.x può visualizzare le statistiche di distribuzione percentuali in modo più semplice rispetto a quando si controllano i singoli contatori di porta con il comando show counters *mod/porta* o con il comando show mac *mod/porta* in CatOS 5.x. Un altro nuovo comando, il comando show channel hash , in CatOS 6.x consente di controllare, in base alla modalità di distribuzione, quale porta verrà selezionata come porta in uscita per determinati indirizzi e/o numeri di porta. I comandi equivalenti per i canali LACP sono il comando show lacp-channel traffic e il comando show lacp-channel hash.

Altre opzioni

Di seguito vengono riportati i possibili passaggi da eseguire se i limiti relativi degli algoritmi basati su MAC Catalyst 4500/4000 o Catalyst 5500/5000 sono un problema e se non si ottiene un buon bilanciamento del carico statistico:

- Switch Catalyst 6500/6000 per installazione point
- Aumentare la larghezza di banda senza effettuare il channeling passando, ad esempio, da diverse porte FE a una porta GE o da più porte GE a una porta 10 GE
- Risolvi coppie di stazioni terminali con flussi di grandi volumi
- Provisioning di collegamenti/VLAN dedicati per dispositivi a elevata larghezza di banda

Linee guida e restrizioni alla configurazione di EtherChannel

EtherChannel verifica le proprietà delle porte su tutte le porte fisiche prima di aggregare le porte compatibili in un'unica porta logica. Le linee guida e le restrizioni alla configurazione variano a seconda della piattaforma dello switch. Seguire le linee guida per evitare problemi di aggregazione. Ad esempio, se QoS è abilitato, EtherChannel non si forma quando si includono i moduli di switching Catalyst serie 6500/6000 con funzionalità QoS diverse. Nel software Cisco IOS, è possibile disabilitare il controllo degli attributi della porta QoS sul bundle EtherChannel con il comando no mls qos channel-consistency interface. Un comando equivalente per disabilitare il controllo degli attributi della porta QoS non è disponibile in CatOS. È possibile usare il comando show port capabilities *mod*/*porta* per visualizzare la funzionalità della porta QoS e determinare se le porte sono compatibili.

Per evitare problemi di configurazione, attenersi alle seguenti linee guida per le diverse piattaforme:

- Sezione *Linee guida per la configurazione di EtherChannel* in Configurazione di EtherChannel (Catalyst 6500/6000)
- Sezione *Linee guida e restrizioni per la configurazione di EtherChannel* in Configurazione di Fast EtherChannel e Gigabit EtherChannel (Catalyst 4500/4000)
- Sezione *Linee guida e restrizioni per la configurazione di EtherChannel* in Configurazione di Fast EtherChannel e Gigabit EtherChannel (Catalyst 5000)

Nota: il numero massimo di canali porte supportati da Catalyst 4000 è 126. Con le versioni software 6.2(1) e precedenti, gli switch Catalyst serie 6500 a sei e nove slot supportano un massimo di 128 EtherChannel. Nel software versione 6.2(2) e successive, la funzione Spanning Tree gestisce l'ID della porta. Pertanto, il numero massimo di EtherChannel con supporto è 126 per uno chassis a sei o nove slot e 63 per uno chassis a 13 slot.

Protocollo Port Aggregation

PAgP è un protocollo di gestione che controlla la coerenza dei parametri a entrambe le estremità del collegamento e assiste il canale nell'adattamento a eventuali errori o aggiunte di collegamenti. Tenere presente quanto segue sulla PAgP:

- PaGP richiede che tutte le porte nel canale appartengano alla stessa VLAN o siano configurate come porte trunk. (Poiché le VLAN dinamiche possono forzare la modifica di una porta in una VLAN diversa, non sono incluse nella partecipazione a EtherChannel.)
- Quando un bundle è già presente e la configurazione di una porta viene modificata (ad esempio, modificando la VLAN o la modalità trunking), tutte le porte nel bundle vengono modificate in base a tale configurazione.
- PAgP non raggruppa le porte che funzionano a velocità diverse o in modalità duplex. Se la velocità e la modalità duplex vengono modificate quando esiste un pacchetto, la modalità PAgP modifica la velocità della porta e la modalità duplex per tutte le porte del pacchetto.

Panoramica operativa

La porta PAgP controlla ogni singola porta fisica o logica da raggruppare. I pacchetti PAgP vengono inviati utilizzando lo stesso indirizzo MAC del gruppo multicast utilizzato per i pacchetti CDP, **01-00-0c-cc-cc-cc**. Il valore del protocollo è 0x0104. Riepilogo dell'operazione del protocollo:

- Finché la porta fisica è `attiva`, i pacchetti PAgP vengono trasmessi ogni secondo durante il rilevamento e ogni 30 secondi in modalità stabile.
- Il protocollo è in ascolto dei pacchetti PAgP che dimostrano che la porta fisica ha una connessione bidirezionale a un altro dispositivo compatibile con PAgP.
- Se si ricevono pacchetti dati ma non pacchetti PAgP, si presume che la porta sia collegata a un dispositivo non compatibile con PAgP.
- Quando due pacchetti PAgP sono stati ricevuti su un gruppo di porte fisiche, tenta di formare una porta aggregata.
- Se i pacchetti PAgP si fermano per un certo periodo di tempo, lo stato PAgP viene `disattivato`.

Elaborazione normale

Per comprendere meglio il comportamento del protocollo, è necessario definire i seguenti concetti:

- **Agport**: una porta logica composta da tutte le porte fisiche nella stessa aggregazione, può essere identificata dal proprio ifIndex SNMP. Pertanto, un agport non contiene porte non operative.
- **Canale**: un'aggregazione che soddisfa i criteri di formazione; potrebbe pertanto contenere porte non operative (gli agport sono un sottoinsieme di canali). I protocolli che includono STP e VTP, ma escludono CDP e DTP, vengono eseguiti sopra la porta PAgP sulle porte agport. Nessuno di questi protocolli può inviare o ricevere pacchetti finché PAgP non collega le proprie porte a una o più porte fisiche.
- **Funzionalità gruppo**: ogni porta fisica e agport possiede un parametro di configurazione denominato funzionalità gruppo. Una porta fisica può essere aggregata a un'altra porta fisica se e solo se hanno la stessa funzionalità di gruppo.
- **Procedura di aggregazione**: quando una porta fisica raggiunge gli stati `UpData` o `UpPAgP`, viene collegata a un agport appropriato. Quando lascia uno di questi stati per un altro stato, viene scollegato dall'agport.

Nella tabella seguente sono riportate le definizioni degli stati e le procedure di creazione:

State	Significato
`SuDati`	Nessun pacchetto PAgP ricevuto. I pacchetti PAgP vengono inviati. La porta fisica è l'unica connessa alla relativa agport. I pacchetti non PAgP vengono trasmessi da una porta fisica all'altra e viceversa.
`Bidirezionale`	È stato ricevuto esattamente un pacchetto PAgP che dimostra l'esistenza di una connessione bidirezionale a un solo router adiacente. La porta fisica non è connessa ad alcuna porta porta secondaria. I pacchetti PAgP vengono inviati e possono essere ricevuti.
`UpPAgP`	Questa porta fisica, probabilmente in associazione con altre porte fisiche, è connessa a una porta di accesso. I pacchetti PAgP vengono inviati e ricevuti sulla porta fisica. I pacchetti non PAgP vengono trasmessi da una porta fisica all'altra e viceversa.

Entrambe le estremità di entrambe le connessioni devono concordare sul tipo di raggruppamento che verrà definito come il gruppo di porte più grande nell'agport consentito da entrambe le estremità della connessione.

Quando una porta fisica raggiunge lo stato `UpPAgP`, viene assegnata all'agport che ha porte fisiche membro che corrispondono alla capacità di gruppo della nuova porta fisica e che si trovano negli stati `BiDir` o `UpPAgP`. (Tutte le porte BiDir di questo tipo vengono spostate contemporaneamente nello stato `UpPAgP`). Se non esiste un agport i cui parametri della porta fisica costitutiva sono compatibili con la porta fisica appena pronta, viene assegnato a un agport con parametri appropriati che non ha porte fisiche associate.

Il timeout PAgP può verificarsi sull'ultimo router adiacente noto sulla porta fisica. Il timeout della porta viene rimosso da agport. Allo stesso tempo, vengono rimosse tutte le porte fisiche sullo

stesso agport i cui timer sono scaduti. In questo modo, un agport la cui altra estremità è morta viene eliminato in una sola volta, anziché una porta fisica alla volta.

Comportamento in caso di errore

Se si verifica un errore nel collegamento di un canale esistente, ad esempio una porta scollegata, la rimozione di Gigabit Interface Converter [GBIC] o il collegamento in fibra interrotto, l'agport viene aggiornato e il traffico viene hashato sui collegamenti rimanenti entro un secondo. Tutto il traffico che non deve essere ripristinato dopo il guasto (traffico che continua a essere inviato sullo stesso collegamento) non subisce alcuna perdita. Il ripristino del collegamento non riuscito attiva un altro aggiornamento dell'agport e l'hashing del traffico viene eseguito di nuovo.

Nota: il comportamento di un collegamento interrotto in un canale a causa di uno spegnimento o della rimozione di un modulo può essere diverso. Per definizione, un canale deve avere due porte fisiche. Se una porta viene persa dal sistema in un canale a due porte, la porta logica viene eliminata e la porta fisica originale viene reinizializzata rispetto allo Spanning Tree. In questo modo, il traffico può essere scartato finché l'STP non consente alla porta di essere di nuovo disponibile per i dati.

Esiste un'eccezione a questa regola sugli switch Catalyst 6500/6000. Nelle versioni precedenti a CatOS 6.3, una porta Agport non viene `eliminata` durante la rimozione del modulo se il canale è composto solo da porte nei moduli 1 e 2.

Questa differenza tra le due modalità di errore è importante quando si pianifica la manutenzione di una rete, in quanto può essere necessario un TCN STP quando si esegue la rimozione o l'inserimento online di un modulo. Come affermato , è importante gestire ogni collegamento fisico nel canale con l'NMS, in quanto l'agport può rimanere indisturbato a causa di un guasto.

Per evitare modifiche indesiderate alla topologia sugli switch Catalyst 6500/6000, si consiglia di effettuare le seguenti operazioni:

- Se per formare un canale si utilizza una singola porta per modulo, è necessario utilizzare tre o più moduli (tre o più porte in totale).
- Se il canale si estende su due moduli, è necessario utilizzare due porte su ciascun modulo (quattro porte in totale).
- Se è necessario un canale a due porte su due schede, utilizzare solo le porte Supervisor Engine.
- Eseguire l'aggiornamento a CatOS 6.3, che gestisce la rimozione dei moduli senza il ricalcolo STP per i canali suddivisi tra i moduli.

Opzioni di configurazione

EtherChannel può essere configurato in modalità diverse, come riepilogato nella tabella seguente:

Modalità	Opzioni configurabili
`On`	PAgP non in funzione. Il channeling della porta è in corso indipendentemente dalla configurazione della porta adiacente. Se la modalità porta adiacente è attiva, viene formato un canale.

Spento	Il channeling della porta non è consentito indipendentemente dalla configurazione della porta adiacente.
Automatico (impostazione predefinita)	L'aggregazione è controllata dal protocollo PAgP. Porta in uno stato di negoziazione passiva e nessun pacchetto PAgP viene inviato sull'interfaccia finché non viene ricevuto almeno un pacchetto PAgP che indica che il mittente funziona in modalità desiderabile.
Desirable	L'aggregazione è controllata dal protocollo PAgP. Porta in uno stato di negoziazione attiva, in cui la porta avvia le negoziazioni con altre porte inviando pacchetti PAgP. Un canale viene formato con un altro gruppo di porte in modalità desiderabile o automatica.
Non-silent (per impostazione predefinita, sulle porte Catalyst 5500/5000 Fiber FE e GE)	Parola chiave auto o mode desiderabile. Se l'interfaccia non riceve pacchetti di dati, non viene mai collegata a un agport e non può essere utilizzata per i dati. Questo controllo della bidirezionalità è stato eseguito su hardware Catalyst 5500/5000 specifico, in quanto alcuni errori di collegamento provocano la divisione del canale. Poiché è attivata la modalità non invisibile all'utente, non è mai consentito a una porta adiacente in fase di ripristino di tornare su e dividere inutilmente il canale. I pacchetti più flessibili e i controlli di bidirezionalità migliorati sono presenti per impostazione predefinita nell'hardware Catalyst serie 4500/4000 e 6500/6000.
Silent (impostazione predefinita su tutte le porte Catalyst 6500/6000 e 4500/4000 e le porte 5500/5000 in	Parola chiave auto o mode desiderabile. Se non si ricevono pacchetti di dati sull'interfaccia, dopo un periodo di timeout di 15 secondi, l'interfaccia viene collegata da sola a un agport e può quindi essere utilizzata per la trasmissione dei dati. La modalità silenziosa consente anche il funzionamento del canale quando il partner può essere un analizzatore o un server che non invia mai PAgP.

rame)	

Le impostazioni `per le connessioni invisibili all'utente/non invisibili all'utente` influiscono sul modo in cui le porte reagiscono a situazioni che causano il traffico unidirezionale o a come raggiungono il failover. Quando una porta non è in grado di trasmettere (ad esempio a causa di un guasto al sottolivello fisico [PHY] o di una fibra o di un cavo interrotti), la porta adiacente può comunque rimanere in stato operativo. Il partner continua a trasmettere i dati, ma questi vanno persi in quanto non è possibile ricevere il traffico di ritorno. Anche i loop Spanning Tree possono formarsi a causa della natura unidirezionale del collegamento.

Alcune porte in fibra hanno la capacità desiderata di portare la porta in uno stato non operativo quando perde il segnale di ricezione (FEFI). In questo modo, la porta del partner non è più operativa e le porte su entrambe le estremità del collegamento non sono più attive.

Se si utilizzano dispositivi che trasmettono dati (ad esempio BPDU) e non sono in grado di rilevare condizioni unidirezionali, è necessario utilizzare la modalità `non silenziosa` per consentire alle porte di rimanere non operative finché non vengono ricevuti i dati e non viene verificato che il collegamento è bidirezionale. Il tempo necessario affinché PAgP rilevi un collegamento unidirezionale è di circa 3,5 * 30 secondi = 105 secondi, dove 30 secondi è il tempo tra due messaggi PAgP successivi. si consiglia l'UDLD come rilevatore più rapido di collegamenti unidirezionali.

Se si utilizzano dispositivi che non trasmettono alcun dato, è necessario utilizzare la modalità `silenziosa`. In questo modo, la porta diventa connessa e operativa indipendentemente dal fatto che i dati ricevuti siano presenti o meno. Inoltre, per le porte in grado di rilevare la presenza di una condizione unidirezionale, ad esempio le piattaforme più recenti che utilizzano L1 FEFI e UDLD, la modalità silenziosa è utilizzata per impostazione predefinita.

Verifica

Nella tabella seguente viene mostrato un riepilogo di tutti i possibili scenari di modalità di channeling PAgP tra due switch connessi direttamente (switch A e switch B). In alcune di queste combinazioni, il protocollo STP può mettere le porte sul lato del channeling nello stato `err-disabled` (ossia, alcune delle combinazioni arrestano le porte sul lato del channeling).

Modalità canale switch A	Modalità canale switch B	Stato canale
`On`	`On`	`Canale` (non PAgP)
`On`	`Spento`	`Non canale` (errdisable)
`On`	`Auto`	`Non canale` (errdisable)
`On`	`Desirable`	`Non canale` (errdisable)
`Spento`	`On`	`Non canale` (errdisable)
`Spento`	`Spento`	`Non canale`
`Spento`	`Auto`	`Non canale`
`Spento`	`Desirable`	`Non canale`
`Auto`	`On`	`Non canale` (errdisable)

Auto	Spento	Non canale
Auto	Auto	Non canale
Auto	Desirable	Canale PAgP
Desirable	On	Non canale (errdisable)
Desirable	Spento	Non canale
Desirable	Auto	Canale PAgP
Desirable	Desirable	Canale PAgP

Suggerimento

Cisco consiglia di abilitare il protocollo PAgP su tutte le connessioni di canale tra switch, evitando la modalità on. Il metodo preferito è impostare la modalità desiderata su entrambe le estremità di un collegamento. Si consiglia inoltre di mantenere la parola chiave silent/non silent sul valore predefinito - silent sugli switch Catalyst 6500/6000 e 4500/4000, non silent sulle porte in fibra Catalyst 5500/5000.

Come accennato in questo documento, la configurazione esplicita del channeling off su tutte le altre porte è utile per l'inoltro rapido dei dati. Evitare di attendere fino a 15 secondi il timeout di PAgP su una porta che non deve essere utilizzata per il channeling, soprattutto perché la porta viene quindi consegnata a STP, che a sua volta può impiegare 30 secondi per consentire l'inoltro dei dati, più potenzialmente 5 secondi per DTP per un totale di 50 secondi. Il comando **set port host** viene descritto più dettagliatamente nella sezione STP di questo documento.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Questo comando assegna ai canali **un** numero di **gruppo amministrativo**, rilevato con un comando **show channel group**. L'aggiunta e la rimozione di porte raggruppate nel canale per la stessa agport possono quindi essere gestite dal numero admin, se lo si desidera.

Altre opzioni

Un'altra configurazione comune per i clienti che dispongono di un modello di amministrazione minima al livello di accesso consiste nell'impostare la modalità su desiderabile ai livelli di distribuzione e di base e lasciare gli switch del livello di accesso alla configurazione automatica predefinita.

Quando si usa il channeling su dispositivi che non supportano PAgP, il canale deve essere hardcoded on (attivato). Ciò è valido per dispositivi come server, director locale, switch di contenuti, router, switch con software precedente, switch Catalyst XL e Catalyst 8540s. Immettere questo comando

```
set port channel port range mode on
```

Il nuovo standard 802.3ad IEEE LACP, disponibile in CatOS 7.x, probabilmente sostituirà PAgP

nel lungo periodo perché offre i vantaggi dell'interoperabilità tra piattaforme e fornitori.

Link Aggregation Control Protocol

Il protocollo LACP è un protocollo che consente alle porte con caratteristiche simili di formare un canale tramite negoziazione dinamica con switch adiacenti. PAgP è un protocollo proprietario di Cisco che può essere eseguito solo sugli switch Cisco e sugli switch rilasciati dai fornitori autorizzati. Tuttavia, il protocollo LACP, definito in IEEE 802.3ad, consente agli switch Cisco di gestire il channeling Ethernet con dispositivi conformi alla specifica 802.3ad. Le versioni software CatOS 7.x hanno introdotto il supporto LACP.

La differenza tra LACP e PAgP da un punto di vista funzionale è minima. Entrambi i protocolli supportano un massimo di otto porte in ciascun canale e le stesse proprietà delle porte vengono controllate prima della formazione del bundle. Queste proprietà delle porte includono:

- Speed
- Duplex
- VLAN nativa
- Tipo trunking

Le differenze notevoli tra LACP e PAgP sono:

- LACP può essere eseguito solo su porte full-duplex e LACP non supporta porte half-duplex.
- LACP supporta porte in standby a caldo. LACP tenta sempre di configurare il numero massimo di porte compatibili in un canale, fino al numero massimo consentito dall'hardware (otto porte). Se il protocollo LACP non è in grado di aggregare tutte le porte compatibili, tutte le porte che non possono essere incluse attivamente nel canale vengono messe in stato di hot standby e utilizzate solo se una delle porte utilizzate si guasta. Un esempio di situazione in cui LACP non è in grado di aggregare tutte le porte compatibili è la presenza di limitazioni hardware più restrittive nel sistema remoto.

Nota: in CatOS, il numero massimo di porte a cui è possibile assegnare la stessa chiave amministrativa è otto. Nel software Cisco IOS, LACP cerca di configurare il numero massimo di porte compatibili in un EtherChannel, fino al numero massimo consentito dall'hardware (otto porte). È possibile configurare otto porte aggiuntive come porte di standby a caldo.

Panoramica operativa

Il protocollo LACP controlla ogni singola porta fisica (o logica) da includere nel pacchetto. I pacchetti LACP vengono inviati con l'indirizzo MAC del gruppo multicast, **01-80-c2-00-00-02**. Il valore del tipo/campo è 0x8809 con un sottotipo di 0x01. Di seguito è riportato un riepilogo dell'operazione del protocollo:

- Il protocollo si basa sui dispositivi per annunciare le loro funzionalità di aggregazione e le informazioni sullo stato. Le trasmissioni sono inviate periodicamente ***su ciascun*** collegamento "aggregabile".
- Finché la porta fisica è attiva, i pacchetti LACP vengono trasmessi ogni secondo durante il rilevamento e ogni 30 secondi in stato stazionario.
- I partner su un collegamento "aggregabile" ascoltano le informazioni inviate all'interno del protocollo e decidono quali azioni intraprendere.
- Le porte compatibili sono configurate in un canale, fino al numero massimo consentito

dall'hardware (otto porte).
- Le aggregazioni sono mantenute grazie allo scambio regolare e tempestivo di informazioni aggiornate sullo stato tra i partner di collegamento. Se la configurazione cambia (ad esempio a causa di un errore nel collegamento), i partner del protocollo scadono e prendono le misure appropriate in base al nuovo stato del sistema.
- Oltre alle trasmissioni periodiche LACP data unit (LACPDU), in caso di modifica delle informazioni sullo stato, il protocollo trasmette al partner una LACPDU basata su eventi. I partner del protocollo prendono le misure appropriate in base al nuovo stato del sistema.

Parametri LACP

Per consentire a LACP di determinare se un insieme di link si connettono allo stesso sistema e se tali link sono compatibili dal punto di vista dell'aggregazione, è necessario poter stabilire questi parametri:

- Identificatore univoco globale per ogni sistema che partecipa all'aggregazione dei collegamentiA ogni sistema che esegue LACP deve essere assegnata una priorità che può essere scelta automaticamente o dall'amministratore. La priorità di sistema predefinita è 32768. La priorità di sistema viene utilizzata principalmente in combinazione con l'indirizzo MAC del sistema per formare l'identificatore di sistema.
- Un mezzo di identificazione dell'insieme di funzionalità associate a ciascuna porta e a ciascun aggregatore, in base alla loro comprensione da parte di un determinato sistemaA ciascuna porta del sistema deve essere assegnata una priorità automaticamente o dall'amministratore. Il valore predefinito è 128. La priorità viene utilizzata insieme al numero di porta per formare l'identificatore della porta.
- Mezzo di identificazione di un gruppo di aggregazione link e del relativo aggregatore associatoLa capacità di una porta di aggregarsi a un'altra porta è riepilogata da un semplice parametro intero a 16 bit rigorosamente maggiore di zero. Questo parametro è denominato "chiave". Ogni chiave è determinata da fattori diversi, ad esempio:Le caratteristiche fisiche delle porte, che comprendono:Velocità datiDuplessitàPoint-to-point o supporto condivisoVincoli di configurazione stabiliti dall'amministratore di reteA ciascuna porta sono associate due chiavi:Chiave amministrativa: consente la manipolazione dei valori delle chiavi da parte della direzione. Un utente può scegliere questa chiave.Una chiave operativa: il sistema utilizza questa chiave per formare le aggregazioni. L'utente non può scegliere o modificare direttamente questa chiave.Il set di porte di un sistema che condividono lo stesso valore di chiave operativa è considerato membro dello stesso gruppo di chiavi.

Se si dispone di due sistemi e di un set di porte con la stessa chiave amministrativa, ogni sistema tenta di aggregare le porte. Ogni sistema inizia dalla porta con la priorità più alta nel sistema con la priorità più alta. Questo comportamento è possibile perché ogni sistema conosce la propria priorità, assegnata dall'utente o dal sistema, e la propria priorità partner, individuata tramite pacchetti LACP.

Comportamento in caso di errore

Il comportamento di errore per LACP è lo stesso di PAgP. Se si verifica un errore in un collegamento di un canale esistente, la porta dell'agport viene aggiornata e il traffico sui collegamenti rimanenti viene bloccato entro un secondo. Un collegamento può avere esito negativo per i motivi seguenti e per altri motivi:

- Una porta è scollegata
- GBIC rimosso
- Una fibra è rotta
- Guasto hardware (interfaccia o modulo)

Tutto il traffico che non deve essere ripristinato dopo il guasto (traffico che continua a essere inviato sullo stesso collegamento) non subisce alcuna perdita. Il ripristino del collegamento non riuscito attiva un altro aggiornamento dell'agport e l'hashing del traffico viene eseguito di nuovo.

Opzioni di configurazione

LACP EtherChannels può essere configurato in modalità diverse, come indicato nella tabella seguente:

Modalità	Opzioni configurabili
`On`	L'aggregazione dei collegamenti deve essere formata senza alcuna negoziazione LACP. Lo switch non invia il pacchetto LACP né elabora alcun pacchetto LACP in arrivo. Se la modalità porta adiacente è `attivata`, viene formato un canale.
`Spento`	La porta non sta effettuando il channeling, a prescindere dalla configurazione della porta adiacente.
`Passivo (predefinito)`	È simile alla modalità `automatica` in PAgP. Lo switch non avvia il canale, ma riconosce i pacchetti LACP in arrivo. Il peer (in stato `attivo`) avvia la negoziazione inviando un pacchetto LACP. Lo switch riceve il pacchetto e risponde a esso, quindi forma il canale di aggregazione con il peer.
`Active`	Questa è simile alla modalità `desiderata` in PAgP. Lo switch avvia la negoziazione per formare un aglink. L'aggregazione dei collegamenti viene formata se l'altra estremità viene eseguita in modalità LACP `attiva` o `passiva`.

Verifica (LACP e LACP)

La tabella riportata in questa sezione mostra un riepilogo di tutti i possibili scenari della modalità di channeling LACP tra due switch connessi direttamente (switch A e switch B). In alcune di queste combinazioni, il protocollo STP può mettere le porte sul lato del channeling nello stato `err-disabled`. Ciò significa che alcune combinazioni chiudono le porte sul lato del channeling.

Modalità canale switch	Modalità canale switch	Stato del canale	Stato canale

A	B	Switch-A	switch B
On	On	Canale (non LACP)	Canale (non LACP)
On	Spento	Non canale (errdisable)	Non canale
On	Passivo	Non canale (errdisable)	Non canale
On	Active	Non canale (errdisable)	Non canale
Spento	Spento	Non canale	Non canale
Spento	Passivo	Non canale	Non canale
Spento	Active	Non canale	Non canale
Passivo	Passivo	Non canale	Non canale
Passivo	Active	Canale LACP	Canale LACP
Active	Active	Canale LACP	Canale LACP

Verifica (LACP e PAgP)

La tabella riportata in questa sezione mostra un riepilogo di tutti i possibili scenari di modalità di channeling da LACP a PAgP tra due switch collegati direttamente (switch A e switch B). In alcune di queste combinazioni, il protocollo STP può mettere le porte sul lato del channeling nello stato `err-disabled`. Ciò significa che alcune combinazioni chiudono le porte sul lato del channeling.

Modalità canale switch A	Modalità canale switch B	Stato del canale Switch-A	Stato canale switch B
On	On	Canale (non LACP)	Canale (non PAgP)
On	Spento	Non canale (errdisable)	Non canale
On	Auto	Non canale (errdisable)	Non canale
On	Desirable	Non canale (errdisable)	Non canale
Spento	On	Non canale	Non canale (errdisable)
Spento	Spento	Non canale	Non canale
Spento	Auto	Non canale	Non canale
Spento	Desirable	Non canale	Non canale
Passivo	On	Non canale	Non canale (errdisable)
Passivo	Spento	Non canale	Non canale
Passivo	Auto	Non canale	Non canale
Passivo	Desirable	Non canale	Non canale
Active	On	Non canale	Non canale (errdisable)
Active	Spento	Non canale	Non canale
Active	Auto	Non canale	Non canale
Active	Desirable	Non canale	Non canale

Suggerimento

Cisco consiglia di abilitare il protocollo PAgP sulle connessioni di canale tra gli switch Cisco. Quando si collegano dispositivi che non supportano PAgP ma supportano LACP, abilitare LACP tramite la configurazione di LACP `attivo` su entrambe le estremità dei dispositivi. Se una delle estremità dei dispositivi non supporta LACP o PAgP, è necessario impostare il codice hardware del canale `su on`.

- **set channelprotocol lacp** *module*

  Sugli switch con CatOS, tutte le porte su Catalyst 4500/4000 e Catalyst 6500/6000 usano il protocollo di canale PAgP per impostazione predefinita e, come tale, non eseguono il protocollo LACP. Per configurare le porte in modo che utilizzino LACP, è necessario impostare il protocollo di canale sui moduli su LACP. Non è possibile eseguire LACP e PAgP sullo stesso modulo sugli switch con CatOS.

- **set port lacp-channel** *port_range admin-key*

  Nel pacchetto LACP viene scambiato un parametro **admin key** (chiave amministrativa). Un canale crea moduli solo tra porte che hanno la stessa chiave di amministrazione. Il comando **set port lacp-channel *port_range admin-key*** assegna ai canali un numero di chiave admin. Il comando **show lacp-channel group** restituisce il numero. Il comando **set port lacp-channel *port_range admin-key*** assegna la stessa chiave admin a tutte le porte dell'intervallo di porte. Se una chiave specifica non è configurata, la chiave admin viene assegnata in modo casuale. Quindi, se si desidera, è possibile fare riferimento alla chiave admin per gestire l'aggiunta e la rimozione delle porte raggruppate nel canale alla stessa agport.

- **set port lacp-channel** *port_range* **mode active**

  Il comando **set port lacp-channel *port_range* mode active** imposta la modalità del canale su `active` per un gruppo di porte a cui era stata precedentemente assegnata la stessa chiave admin.

Inoltre, LACP utilizza un timer a intervalli di 30 secondi (Slow_Periodic_Time) dopo la definizione dei canali EtherLACP. Il numero di secondi prima dell'annullamento della convalida delle informazioni LACPDU ricevute con l'uso di timeout lunghi (3 x Slow_Periodic_Time) è 90. Usare UDLD, un rilevatore più rapido di collegamenti unidirezionali. Non è possibile regolare i timer LACP e oggi non è possibile configurare gli switch in modo che utilizzino la trasmissione PDU veloce (ogni secondo) per mantenere il canale dopo che è stato formato.

Altre opzioni

Se disponete di un modello di amministrazione minima al livello di accesso, una configurazione comune consiste nell'impostare la modalità su `attiva` ai livelli di distribuzione e di base. Lasciare gli switch del livello di accesso nella configurazione `passiva` predefinita.

Rilevamento collegamenti unidirezionali

UDLD è un protocollo leggero e proprietario di Cisco sviluppato per rilevare le istanze di comunicazioni unidirezionali tra i dispositivi. Sebbene esistano altri metodi per rilevare lo stato bidirezionale dei mezzi di trasmissione, come FEFI, in alcuni casi i meccanismi di rilevamento L1 non sono sufficienti. Questi scenari possono determinare una delle situazioni seguenti:

- Il funzionamento imprevedibile di STP
- Inondazione errata o eccessiva dei pacchetti
- Il buco nero del traffico

La funzionalità UDLD è progettata per risolvere le seguenti condizioni di errore sulle interfacce Ethernet in fibra e in rame:

- Monitorare le configurazioni del cablaggio fisico e arrestare le porte con cavi errati per `disabilitarle`.
- Protezione da collegamenti unidirezionali. Quando viene rilevato un collegamento unidirezionale, a causa di un malfunzionamento del supporto o della porta/interfaccia, la porta interessata viene chiusa e `disabilitata a causa di` un errore, quindi viene generato un messaggio syslog corrispondente.
- Inoltre, la modalità aggressiva UDLD controlla che un collegamento precedentemente ritenuto bidirezionale non perda la connettività durante la congestione e non sia più utilizzabile. UDLD esegue test di connettività continui sul collegamento. Lo scopo principale della modalità aggressiva UDLD è quello di evitare il black holing del traffico in alcune condizioni di errore.

Spanning Tree, con il suo flusso BPDU unidirezionale allo stato stazionario, è stato un grave malato di questi errori. È facile capire come una porta possa improvvisamente non essere in grado di trasmettere le BPDU, causando una modifica dello stato di STP da `blocco` a `inoltro` sul router adiacente. Questa modifica crea un loop, poiché la porta è ancora in grado di ricevere.

Panoramica operativa

UDLD è un protocollo L2 che opera sul layer LLC (destinazione MAC 01-00-0c-cc-cc-cc, tipo di protocollo SNAP HDLC 0x0111). Quando si esegue UDLD in combinazione con i meccanismi FEFI e di negoziazione automatica L1, è possibile convalidare l'integrità fisica (L1) e logica (L2) di un collegamento.

UDLD offre funzionalità e protezione che FEFI e la funzione di negoziazione automatica non sono in grado di eseguire, ossia il rilevamento e la memorizzazione nella cache di informazioni sui router adiacenti, la capacità di disattivare porte non collegate in modo corretto e il rilevamento di malfunzionamenti o errori di porte e interfacce logiche su collegamenti non point-to-point (ossia coloro che attraversano convertitori di supporti o hub).

il protocollo UDLD utilizza due meccanismi di base; viene appresa la conoscenza dei router adiacenti e mantiene le informazioni aggiornate in una cache locale e invia una serie di messaggi di avviso/risposta (hello) UDLD ogni volta che rileva un nuovo router adiacente o ogni volta che un router adiacente richiede una risincronizzazione della cache.

UDLD invia costantemente messaggi di richiesta su tutte le porte su cui UDLD è abilitato. Ogni volta che si riceve un messaggio UDLD "triggering" specifico su una porta, viene avviata una fase di rilevamento e un processo di convalida. Se al termine di questo processo tutte le condizioni valide sono soddisfatte, lo stato della porta non viene modificato. Per soddisfare le condizioni, la porta deve essere bidirezionale e correttamente cablata. In caso contrario, la porta è `disabilitata a causa di un errore` e viene visualizzato un messaggio syslog. Il messaggio syslog è simile ai seguenti messaggi:

- `UDLD-3-DISABLE: Rilevato collegamento unidirezionale sulla porta [dec]/[dec]. Porta disabilitata`
- `UDLD-4-ONEWAYPATH: Un collegamento unidirezionale dalla porta [dec]/[dec] alla porta Rilevato [dec]/[dec] della periferica [chars]`

Per un elenco completo dei messaggi di sistema per struttura, che include eventi UDLD, fare riferimento a Messaggi e procedure di recupero (switch Catalyst serie 7.6).

Dopo aver stabilito un collegamento e averlo classificato come bidirezionale, UDLD continua a pubblicizzare i messaggi probe/echo a un intervallo predefinito di 15 secondi. Questa tabella rappresenta gli stati del collegamento UDLD validi come riportato nell'output del comando **show udld port**:

Stato porta	Commento
Indeterminato	Rilevamento in corso, un'entità UDLD adiacente è stata disabilitata o la trasmissione è stata bloccata.
Non applicabile	UDLD disabilitato.
Shutdown	È stato rilevato un collegamento unidirezionale e la porta è stata disabilitata.
Bidirezionale	È stato rilevato un collegamento bidirezionale.

- **Manutenzione cache adiacente**: UDLD invia periodicamente pacchetti echo/probe su ogni interfaccia attiva per mantenere l'integrità della cache dei nodi adiacenti UDLD. Ogni volta che si riceve un messaggio hello, questo viene memorizzato nella cache e conservato in memoria per un periodo massimo definito come tempo di attesa. Alla scadenza del tempo di attesa, la voce della cache corrispondente viene esaurita. Se viene ricevuto un nuovo messaggio di saluto entro il periodo di tempo di attesa, il nuovo messaggio sostituisce quello precedente e il timer di durata corrispondente viene reimpostato.
- Per mantenere l'integrità della cache UDLD, quando un'interfaccia abilitata per il protocollo UDLD viene disabilitata o un dispositivo viene reimpostato, tutte le voci della cache esistenti per le interfacce interessate dalla modifica della configurazione vengono cancellate e UDLD trasmette almeno un messaggio per informare i rispettivi vicini di scaricare le voci della cache corrispondenti.
- **Meccanismo di rilevamento dell'eco** - il meccanismo di eco forma la base dell'algoritmo di rilevamento. Ogni volta che un dispositivo UDLD viene a conoscenza di un nuovo router adiacente o riceve una richiesta di risincronizzazione da un router adiacente non sincronizzato, avvia/riavvia la finestra di rilevamento sul lato della connessione e invia una sequenza di messaggi echo in risposta. Poiché questo comportamento deve essere lo stesso per tutti i router adiacenti, il mittente dell'eco si aspetta di ricevere un'altra risposta. Se la finestra di rilevamento termina e non è stato ricevuto alcun messaggio di risposta valido, il collegamento viene considerato unidirezionale e può essere avviato un processo di riattivazione del collegamento o di arresto della porta.

Tempo di convergenza

Per evitare loop di tipo STP, CatOS 5.4(3) ha ridotto l'intervallo dei messaggi predefinito UDLD da 60 secondi a 15 secondi al fine di arrestare un collegamento unidirezionale prima che una porta bloccata potesse passare a uno stato di inoltro.

Nota: il valore dell'intervallo tra i messaggi determina la frequenza con cui un router adiacente invia le sonde UDLD dopo la fase di collegamento o rilevamento. Non è necessario che l'intervallo tra i messaggi corrisponda su entrambe le estremità di un collegamento, anche se è preferibile una configurazione coerente quando possibile. Quando si stabiliscono i router adiacenti UDLD, viene inviato l'intervallo di messaggi configurato e viene calcolato l'intervallo di timeout per il peer (3 * message_interval). Di conseguenza, una relazione peer si interrompe dopo che tre hellop (o sonde) consecutivi sono mancanti. Con intervalli di messaggi diversi su ciascun lato, questo valore di timeout è diverso su ciascun lato.

Il tempo approssimativo necessario affinché UDLD rilevi un errore unidirezionale è circa (2,5 * intervallo_messaggi + 4 secondi), o circa 41 secondi con l'intervallo predefinito di 15 secondi. Questo valore è ben al di sotto dei 50 secondi solitamente necessari per la riconversione di STP. Se la CPU NMP dispone di alcuni cicli di riserva e se si controlla attentamente il livello di utilizzo, è possibile ridurre l'intervallo (pari) dei messaggi al minimo di 7 secondi. Questo intervallo di messaggi consente di velocizzare il rilevamento in base a un fattore significativo.

Di conseguenza, il protocollo UDLD dipende dai timer Spanning Tree predefiniti. Se si sintonizza STP per una convergenza più rapida rispetto a UDLD, prendere in considerazione un meccanismo alternativo, ad esempio la funzione di protezione del loop CatOS 6.2. Quando si implementa RSTP (IEEE 802.1w), prendere in considerazione anche un meccanismo alternativo in quanto RSTP ha caratteristiche di convergenza in millisecondi, che dipendono dalla topologia. In questi casi, utilizzare la funzione di protezione loop insieme al protocollo UDLD, che offre la massima protezione. La funzione Loop Guard impedisce che i loop STP vengano eseguiti alla velocità della versione STP in uso e UDLD rileva connessioni unidirezionali sui singoli collegamenti EtherChannel o nei casi in cui le BPDU non fluiscono lungo la direzione interrotta.

Nota: il protocollo UDLD non rileva tutte le situazioni di errore dell'STP, ad esempio gli errori causati da una CPU che non invia pacchetti BPDU per un tempo superiore a (2 * FwdDelay + Maxage). Per questo motivo, Cisco consiglia di implementare il protocollo UDLD insieme a loop guard (introdotto in CatOS 6.2) nelle topologie che si basano sul protocollo STP.

Attenzione: prestare attenzione alle versioni precedenti di UDLD che usano un intervallo di messaggi predefinito non configurabile di 60 secondi. Queste versioni possono essere soggette a condizioni di loop nello spanning-tree.

Modalità UDLD Aggressive

Il protocollo UDLD aggressivo è stato creato per risolvere quei (pochi) casi in cui è necessario un test continuo della connettività bidirezionale. Pertanto, la modalità aggressiva offre una protezione avanzata contro le condizioni di collegamento unidirezionale pericolose in queste situazioni:

- Quando la perdita di PDU UDLD è simmetrica e le due porte scadono, nessuna delle due viene disabilitata a causa di un errore.
- Un lato del collegamento ha una porta bloccata (entrambe le porte trasmettono [Tx] e Rx).
- Un lato del collegamento rimane attivo mentre l'altro lato è inattivo.
- La negoziazione automatica o un altro meccanismo di rilevamento degli errori L1 è disabilitato.
- Èauspicabile una riduzione del ricorso ai meccanismi FEFI L1.
- Ènecessaria la massima protezione da errori di collegamento unidirezionale su collegamenti FE/GE point-to-point. In particolare, quando non è ammesso alcun guasto tra due vicini, le sonde aggressive rispetto al protocollo UDLD possono essere considerate un "battito

cardiaco", la cui presenza garantisce la salute del collegamento.

Il caso più comune di implementazione di un protocollo UDLD aggressivo è quello di eseguire il controllo della connettività su un membro di un bundle quando la negoziazione automatica o un altro meccanismo di rilevamento degli errori L1 è disabilitato o inutilizzabile. Ciò è particolarmente vero con le connessioni EtherChannel perché PAgP/LACP, anche se abilitato, non usa timer di benvenuto molto bassi allo stato stazionario. In questo caso, l'UDLD aggressivo ha l'ulteriore vantaggio di prevenire possibili loop nello spanning-tree.

Le circostanze che contribuiscono alla perdita simmetrica dei pacchetti della sonda UDLD sono più difficili da caratterizzare. È necessario comprendere che il protocollo UDLD normale verifica la presenza di una condizione di collegamento unidirezionale, anche quando un collegamento raggiunge lo stato bidirezionale. Lo scopo del protocollo UDLD è rilevare i problemi L2 che causano loop STP e tali problemi sono in genere unidirezionali in quanto il flusso delle BPDU viene eseguito solo in una direzione allo stato stazionario. Pertanto, l'uso del protocollo UDLD normale insieme alla negoziazione automatica e alla protezione in loop (per le reti che si basano sul protocollo STP) è quasi sempre sufficiente. Tuttavia, la modalità aggressiva UDLD è utile nelle situazioni in cui la congestione è influenzata nello stesso modo in entrambe le direzioni, causando la perdita di richieste UDLD in entrambe le direzioni. Ad esempio, questa perdita di richieste UDLD può verificarsi se l'utilizzo della CPU su ciascuna estremità del collegamento è elevato. Altri esempi di perdita bidirezionale della connettività includono il guasto di uno di questi dispositivi:

- Transponder DWDM (Dense Wavelength Division Multiplexing)
- Un convertitore multimediale
- Un hub
- Un altro dispositivo L1**Nota:** l'errore non può essere rilevato dalla negoziazione automatica.

Un errore UDLD aggressivo disabilita la porta in queste situazioni di errore. Considerare attentamente le ramificazioni quando si abilita la modalità aggressiva UDLD sui collegamenti non point-to-point. I collegamenti con convertitori di supporti, hub o dispositivi simili non sono point-to-point. I dispositivi intermedi possono impedire l'inoltro di pacchetti UDLD e forzare la chiusura innecessaria di un collegamento.

Dopo il timeout di tutte le porte adiacenti, la modalità aggressiva UDLD (se abilitata) riavvia la sequenza di collegamento nel tentativo di eseguire una risincronizzazione con tutte le porte adiacenti potenzialmente non sincronizzate. Questa operazione viene eseguita nella fase di annuncio o di rilevamento. Se, dopo una trasmissione rapida dei messaggi (otto tentativi non riusciti), il collegamento viene comunque considerato "indeterminato", la porta viene messa in stato `err-disabled`.

Nota: alcuni switch non supportano il protocollo UDLD. Attualmente, Catalyst 2900XL e Catalyst 3500XL dispongono di intervalli di messaggi hardcoded di 60 secondi. Questo intervallo non è considerato sufficientemente veloce da proteggere da potenziali loop STP (con l'uso dei parametri STP predefiniti).

UDLD su collegamenti indirizzati

Ai fini di questa discussione, un link indirizzato è uno dei due tipi di connessione seguenti:

- Point-to-point tra due nodi di routerQuesto collegamento è configurato con una subnet mask a 30 bit.
- Una VLAN con più porte ma che supporta solo connessioni indirizzateUn esempio è una topologia di base L2 divisa.

Ciascun protocollo IGRP (Interior Gateway Routing Protocol) ha caratteristiche univoche per quanto riguarda il modo in cui gestisce le relazioni tra nodi adiacenti e la convergenza dei percorsi. Le caratteristiche descritte in questa sezione sono significative quando si contrappongono due dei protocolli di routing più diffusi attualmente in uso, il protocollo OSPF (Open Shortest Path First) e l'EIGRP (Enhanced IGRP).

In primo luogo, si noti che un guasto L1 o L2 su una rete con routing point-to-point determina la disattivazione quasi immediata della connessione L3. Poiché l'unica porta dello switch della VLAN passa a uno stato non connesso in seguito a un errore L1/L2, la funzione di stato automatico dell'MSFC sincronizza gli stati delle porte L2 e L3 in circa due secondi. Questa sincronizzazione attiva l'interfaccia VLAN L3/down (con il protocollo di linea non attivo).

Valori del timer predefiniti. OSPF invia messaggi di benvenuto ogni 10 secondi e ha un intervallo inattivo di 40 secondi (4 * salve). Questi timer sono coerenti per le reti point-to-point e broadcast OSPF. Poiché per formare un adiacente OSPF richiede una comunicazione bidirezionale, il tempo di failover peggiore è di 40 secondi. Questo failover avviene anche se il guasto di L1/L2 non è solo su una connessione point-to-point, lasciando uno scenario parzialmente operativo che deve essere gestito dal protocollo L3. Poiché il tempo di rilevamento del protocollo UDLD è molto simile al tempo di un timer inattivo OSPF che scade (circa 40 secondi), i vantaggi della configurazione della modalità normale UDLD su un collegamento point-to-point OSPF L3 sono limitati.

In molti casi, la convergenza EIGRP è più rapida rispetto alla tecnologia OSPF. Tuttavia, non è necessario stabilire una comunicazione bidirezionale perché i vicini possano scambiarsi le informazioni di routing. In scenari di guasto semoperazionale molto specifici, EIGRP è vulnerabile al blocco nero del traffico che dura fino a quando qualche altro evento rende i percorsi attraverso quel vicino "attivo". La modalità normale UDLD può ridurre le circostanze descritte in questa sezione. La modalità normale UDLD rileva un errore nel collegamento unidirezionale e la porta viene disabilitata a causa di un errore.

Per le connessioni con routing L3 che usano un protocollo di routing qualsiasi, UDLD normal assicura la protezione contro i problemi al momento dell'attivazione iniziale del collegamento. Tali problemi includono cablaggio errato o hardware difettoso. Inoltre, la modalità aggressiva UDLD offre i seguenti vantaggi sulle connessioni con routing L3:

- Impedisce inutili blocchi del traffico**Nota:** in alcuni casi sono necessari timer minimi.
- Attiva lo stato `err-disabled` per il collegamento intermittente
- Protezione da loop risultanti da configurazioni EtherChannel L3

Comportamento predefinito del protocollo UDLD

Il protocollo UDLD è disabilitato a livello globale e abilitato per impostazione predefinita nelle porte Fibre Channel. Poiché il protocollo UDLD è un protocollo di infrastruttura necessario solo tra switch, per impostazione predefinita il protocollo UDLD è disabilitato sulle porte in rame. Le porte in rame vengono in genere utilizzate per l'accesso host.

Nota: per poter ottenere lo stato bidirezionale dei router adiacenti, il protocollo UDLD deve essere abilitato a livello globale e a livello di interfaccia. In CatOS 5.4(3) e versioni successive, l'intervallo predefinito per i messaggi è 15 secondi ed è configurabile tra 7 e 90 secondi.

Il ripristino della porta da una condizione di errore è disabilitato a livello globale per impostazione predefinita. Dopo essere stata abilitata a livello globale, se una porta entra in stato `err-disabled`, la porta viene riabilitata automaticamente dopo un intervallo di tempo selezionato. L'ora predefinita è

300 secondi, un timer globale che viene mantenuto per tutte le porte di uno switch. Se il timeout di errdisable per la porta è stato impostato su `disable`, è possibile impedire manualmente la riattivazione della porta. Eseguire il **comando set port errdisable-timeout *mod*/*porta disable***.

Nota: l'uso di questo comando dipende dalla versione del software in uso.

Prendere in considerazione l'uso della funzione di timeout di errdisable quando si implementa la modalità aggressiva UDLD senza funzionalità di gestione della rete fuori banda, in particolare sul livello di accesso o su qualsiasi dispositivo che possa rimanere isolato dalla rete in caso di errore.

Per ulteriori informazioni su come configurare un periodo di timeout per le porte in stato `err-disabled`, consultare il documento sulla configurazione dello switching Ethernet, Fast Ethernet, Gigabit e 10 Gigabit Ethernet.

Suggerimento

Nella maggior parte dei casi, il protocollo UDLD in modalità normale è sufficiente se usato correttamente insieme alle funzionalità e ai protocolli appropriati. Le caratteristiche/protocolli includono:

- FEFI
- Negoziazione automatica
- Protezione loop

Quando si distribuisce il protocollo UDLD, valutare se è necessario un test continuo della connettività bidirezionale (modalità aggressiva). In genere, se la negoziazione automatica è abilitata, la modalità aggressiva non è necessaria perché la negoziazione automatica compensa il rilevamento degli errori a L1.

Cisco consiglia di abilitare la modalità normale UDLD su tutti i collegamenti FE/GE point-to-point tra gli switch Cisco in cui l'intervallo dei messaggi UDLD è impostato sull'impostazione predefinita di 15 secondi. In questa configurazione si presuppongono i timer Spanning Tree 802.1d predefiniti. Inoltre, utilizzare il protocollo UDLD insieme alla protezione loop nelle reti che si basano sul protocollo STP per la ridondanza e la convergenza. Questa raccomandazione si applica alle reti in cui vi sono una o più porte in stato di blocco STP nella topologia.

Per abilitare il protocollo UDLD, eseguire questi comandi:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set
udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

Le porte disabilitate a causa di sintomi di collegamento unidirezionale devono essere abilitate manualmente. Eseguire il comando **set port enable**.

Per ulteriori informazioni, fare riferimento a Descrizione e configurazione della funzionalità UDLD (Unidirectional Link Detection Protocol).

Altre opzioni

Per la massima protezione dai sintomi derivanti da collegamenti unidirezionali, configurare il

protocollo UDLD in modalità aggressiva:

```
set udld aggressive-mode enable port_range
```

Inoltre, è possibile regolare il valore dell'intervallo dei messaggi UDLD tra 7 e 90 secondi a ciascuna estremità, se supportato, per ottenere una convergenza più rapida:

```
set udld interval time
```

Prendere in considerazione l'uso della funzione di timeout di errdisable su qualsiasi dispositivo che possa rimanere isolato dalla rete in caso di situazione di errdisable. Questa situazione si verifica in genere nel livello di accesso e quando si implementa la modalità aggressiva UDLD senza funzionalità di gestione della rete fuori banda.

Se una porta è in stato `err-disabled`, per impostazione predefinita la porta rimane inattiva. È possibile usare questo comando per riattivare le porte dopo un intervallo di timeout:

Nota: per impostazione predefinita, l'intervallo di timeout è 300 secondi.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Se il dispositivo partner non è compatibile con UDLD, ad esempio un host finale o un router, non eseguire il protocollo. Immettere questo comando

```
set udld disable port_range
```

Test e monitoraggio UDLD

Il protocollo UDLD non è facile da testare senza un componente realmente difettoso/unidirezionale presente in laboratorio, ad esempio un GBIC difettoso. Il protocollo è stato progettato per rilevare scenari di errore meno comuni rispetto agli scenari generalmente utilizzati in un laboratorio. Ad esempio, se si esegue un test semplice e si scollega un trefolo di una fibra per verificare lo stato `err-disabled` desiderato, è necessario aver disattivato la negoziazione automatica L1. In caso contrario, la porta fisica si spegne e la comunicazione del messaggio UDLD viene reimpostata. L'estremità remota passa allo stato indeterminato in modalità UDLD normale. Se si utilizza la modalità aggressiva UDLD, l'estremità remota viene messa nello stato `err-disabled`.

Èdisponibile un metodo di test aggiuntivo per simulare la perdita di PDU nei sistemi adiacenti per il protocollo UDLD. Usare i filtri del livello MAC per bloccare l'indirizzo hardware UDLD/CDP e permettere il passaggio di altri indirizzi.

Per monitorare il protocollo UDLD, usare i seguenti comandi:

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds


>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1      enabled       disabled         bidirectional
```

Anche dalla modalità `abilitazione`, è possibile usare il comando nascosto show udld neighbors per controllare il contenuto della cache UDLD (come accade con il CDP). Spesso è utile confrontare la cache UDLD con la cache CDP per verificare se esiste un'anomalia specifica del protocollo. Ogni volta che viene influenzato anche il CDP, tutte le PDU/BPDU sono in genere interessate. Pertanto, selezionare anche STP. Ad esempio, verificare se sono state apportate modifiche recenti all'identità principale o alla posizione della porta principale/designata.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

Inoltre, è possibile monitorare lo stato UDLD e la coerenza della configurazione utilizzando le variabili MIB UDLD SNMP di Cisco.

Frame jumbo

La dimensione predefinita del frame MTU (Maximum Transmission Unit) è di 1518 byte per tutte le porte Ethernet, incluse le porte GE e 10 GE. La funzione jumbo frame consente alle interfacce di commutare frame più grandi della dimensione standard Ethernet. Questa funzione è utile per ottimizzare le prestazioni da server a server e per supportare applicazioni quali MPLS (Multi-Protocol Label Switching), tunneling 802.1Q e L2TPv3 (L2 Tunneling Protocol versione 3), che aumentano le dimensioni dei frame originali.

Panoramica operativa

La specifica dello standard IEEE 802.3 definisce una dimensione massima del frame Ethernet di 1518 byte per i frame normali e di 1522 byte per i frame 802.1Q incapsulati. I frame incapsulati 802.1Q sono talvolta chiamati "baby giants". In generale, i pacchetti vengono classificati come frame giant quando superano la lunghezza massima Ethernet specificata per una connessione Ethernet specifica. I pacchetti giganti sono anche noti come frame jumbo.

Ci sono diversi motivi per cui le dimensioni MTU di alcuni frame possono superare i 1518 byte. Ecco alcuni esempi:

- Requisiti specifici del fornitore: le applicazioni e alcune schede NIC possono specificare una dimensione MTU non compresa nei 1500 byte standard. La tendenza a specificare tali dimensioni MTU si basa sugli studi intrapresi, che provano che un aumento delle dimensioni di un frame Ethernet può aumentare il throughput medio.
- Trunking: per trasportare le informazioni sull'ID VLAN tra gli switch o altri dispositivi di rete, il

trunking è stato impiegato per aumentare il frame Ethernet standard. Oggi, le due forme più comuni di trunking sono l'incapsulamento ISL di proprietà di Cisco e IEEE 802.1Q.
- MPLS - Quando MPLS è abilitato su un'interfaccia, può aumentare le dimensioni del frame di un pacchetto. Questo aumento dipende dal numero di etichette nello stack per un pacchetto con tag MPLS. La dimensione totale di un'etichetta è di 4 byte. La dimensione totale di uno stack di etichette è *n* x 4 byte. Se è formato uno stack di etichette, i frame possono superare l'MTU.
- Tunneling 802.1Q: i pacchetti di tunneling 802.1Q contengono due tag 802.1Q, di cui in genere è visibile solo un tag alla volta per l'hardware. Pertanto, il tag interno aggiunge 4 byte al valore MTU (dimensioni del payload).
- Universal Transport Interface (UTI)/L2TPv3—UTI/L2TPv3 incapsula i dati L2 che devono essere inoltrati sulla rete IP. L'incapsulamento può aumentare le dimensioni del frame originale fino a 50 byte. Il nuovo frame include una nuova intestazione IP (20 byte), un'intestazione L2TPv3 (12 byte) e una nuova intestazione L2. Il payload L2TPv3 è costituito dal frame L2 completo, che include l'intestazione L2.

La capacità dei diversi switch Catalyst di supportare varie dimensioni di frame dipende da molti fattori, tra cui l'hardware e il software. Alcuni moduli possono supportare frame di dimensioni maggiori rispetto ad altri, anche all'interno della stessa piattaforma.

- Gli switch Catalyst 5500/5000 supportano i frame jumbo in CatOS 6.1. Quando la funzione jumbo frame è abilitata su una porta, le dimensioni dell'MTU aumentano a 9216 byte. Sulle schede di linea basate su UTP (unshielded twisted pair) con velocità di 10/100 Mbps, la dimensione massima del frame supportata è solo 8092 byte. Questa limitazione è una limitazione ASIC. Generalmente non ci sono restrizioni nell'attivazione della funzione di dimensione del frame jumbo. Questa funzione può essere utilizzata con i comandi trunking/non trunking e channeling/non channeling.
- Gli switch Catalyst 4000 (Supervisor Engine 1 [WS-X4012] e Supervisor Engine 2 [WS-X4013]) non supportano i frame jumbo a causa di una limitazione ASIC. Tuttavia, l'eccezione è rappresentata dal trunking 802.1Q.
- La piattaforma Catalyst serie 6500 può supportare frame di dimensioni jumbo in CatOS versione 6.1(1) e successive. Tuttavia, questo supporto dipende dal tipo di schede di linea utilizzate. Generalmente non ci sono restrizioni nell'attivazione della funzione di dimensione del frame jumbo. Questa funzione può essere utilizzata con i comandi trunking/non trunking e channeling/non channeling. La dimensione MTU predefinita è 9216 byte dopo che il supporto dei frame jumbo è stato abilitato sulla singola porta. L'MTU predefinita non è configurabile con CatOS. Tuttavia, il software Cisco IOS versione 12.1(13)E ha introdotto il comando **system jumbomtu** per sostituire l'MTU predefinita.

per ulteriori informazioni, fare riferimento al supporto di frame jumbo/gigante sugli switch Catalyst.

Nella tabella seguente vengono descritte le dimensioni MTU supportate dalle diverse schede di linea per gli switch Catalyst serie 6500/6000:

Nota: le dimensioni MTU o il pacchetto si riferiscono solo al payload Ethernet.

Scheda di linea	Dimensioni MTU
Predefinito	9216 byte

WS-X6248-RJ-45, WS-X6248A-RJ-45 WS-X6248-TEL, WS-X6248A-TEL WS-X6348-RJ-45(V), WS-X6348-RJ-21(V)	8092 byte (limitati dal chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100 byte (@ 100 Mbps) 9216 byte (@ 10 Mbps)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216 byte
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216 byte
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45AF WS-X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, X6316-GE-TX , WS-X6416-GBIC WS-X6516-GBIC, WS-X6516A-GBIC, WS-X6816-GBIC Uplink di Supervisor Engine 1, 2, 32 e 720	9216 byte
WS-X6516-GE-TX	8092 byte (@ 100 Mbps) 9216 byte (@ 10 o 1000 Mbps)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF	1500 byte (frame jumbo non supporta to)
Serie WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx	9216 byte
OSM ATM (OC12c)	9180 byte
OSM CHOC3, CHOC12, CHOC48, CT3	9216 byte (OCx e DS3) 7673 byte (T1/E1)

Flex WAN	7673 byte (CT3 T1/DS0) 9216 byte (OC3c POS) 7673 byte (T1)
CSM (WS-X606-SLB-APC)	9216 byte (di CSM 3.1(5) e 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, OSM GE WAN	9216 byte

Supporto frame jumbo di layer 3

Con CatOS in esecuzione sul Supervisor Engine e il software Cisco IOS in esecuzione sull'MSFC, gli switch Catalyst 6500/6000 offrono anche il supporto di frame jumbo L3 nel software Cisco IOS® versione 12.1(2)E e successive con l'utilizzo di hardware PFC/MSFC2, PFC2/MSFC2 o versioni successive. Se le VLAN in entrata e in uscita sono configurate entrambe per i frame jumbo, tutti i pacchetti vengono commutati dall'hardware dal PFC alla velocità wire. Se la VLAN in entrata è configurata per i frame jumbo e la VLAN in uscita non è configurata, vi sono due scenari:

- Un jumbo frame inviato dall'host finale con il bit "non frammentare" (DF, Don't Fragment) impostato (per il rilevamento della MTU del percorso). Il pacchetto viene scartato e un messaggio ICMP (Internet Control Message Protocol) non raggiungibile viene inviato all'host finale con il `frammento di` codice del messaggio `necessario e il DF impostato`.
- Frame jumbo inviato dall'host finale con bit DF non impostato. I pacchetti vengono frammentati su MSFC2/MSFC3 e quindi inseriti nel software.

La tabella fornisce un riepilogo del supporto jumbo L3 per diverse piattaforme:

Switch o modulo L3	**Dimensioni massime MTU L3**
Catalyst serie 2948G-L3/4908G-L3	I frame jumbo non sono supportati.
Catalyst 5000 RSM[1]/RSFC[2]	I frame jumbo non sono supportati.
Catalyst 6500 MSFC1	I frame jumbo non sono supportati.
Catalyst 6500 MSFC2 e versioni successive	Software Cisco IOS release 12.1(2)E: 9216 byte

[1] RSM = Route Switch Module

[2] RSFC = Route Switch Feature Card

Considerazioni sulle prestazioni della rete

Le prestazioni di TCP su WAN (Internet) sono state studiate in modo approfondito. Questa equazione spiega come il throughput TCP abbia un limite superiore basato su:

- Il valore Maximum Segment Size (MSS), ossia la lunghezza dell'MTU meno la lunghezza delle intestazioni TCP/IP
- Round Trip Time (RTT)
- La perdita di pacchetti

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

In base a questa formula, la velocità di trasmissione TCP massima raggiungibile è direttamente proporzionale al valore MSS. Con il routing RTT costante e la perdita di pacchetti, è possibile raddoppiare la velocità di trasmissione TCP raddoppiando le dimensioni del pacchetto. Analogamente, quando si utilizzano frame jumbo anziché frame da 1518 byte, un aumento di dimensioni pari a sei volte può comportare un potenziale miglioramento di sei volte nella velocità TCP di una connessione Ethernet.

In secondo luogo, le crescenti esigenze di prestazioni delle server farm richiedono un mezzo più efficiente per garantire velocità di trasferimento dati più elevate con i datagrammi UDP NFS (Network File System). NFS è il meccanismo di storage dei dati più diffuso per il trasferimento di file tra server basati su UNIX e offre datagrammi da 8400 byte. Data l'MTU estesa di 9 KB di Ethernet, un singolo jumbo frame è abbastanza grande da avere un datagramma dell'applicazione di 8 KB (ad esempio, NFS) più il sovraccarico dell'intestazione del pacchetto. Questa funzionalità consente, tra l'altro, trasferimenti DMA (Direct Memory Access) più efficienti sugli host, in quanto il software non ha più bisogno di frammentare i blocchi NFS in datagrammi UDP separati.

Suggerimento

Se si desidera il supporto dei frame jumbo, limitare l'uso dei frame jumbo alle aree della rete in cui tutti i moduli di switch (L2) e le interfacce (L3) supportano i frame jumbo. Questa configurazione impedisce la frammentazione in qualsiasi punto del percorso. La configurazione di frame jumbo di lunghezza superiore a quella supportata nel percorso elimina i vantaggi derivanti dall'uso della funzione, in quanto è necessaria la frammentazione. Come mostrano le tabelle in questa sezione Jumbo Frame, le diverse piattaforme e schede di linea possono variare in base alle dimensioni massime dei pacchetti supportate.

Configurare i dispositivi host jumbo compatibili con il frame con una MTU delle dimensioni minime corrispondenti al denominatore comune supportato dall'hardware di rete, per l'intera VLAN L2 in cui risiede il dispositivo host. Per abilitare il supporto jumbo frame per i moduli con supporto jumbo frame, eseguire questo comando:

```
set port jumbo mod/port enable
```

Inoltre, se si desidera il supporto di jumbo frame oltre i limiti della rete L3, configurare il valore MTU più grande disponibile di 9216 byte su tutte le interfacce VLAN applicabili. Usare il comando **mtu** nelle interfacce VLAN:

```
interface vlan vlan# mtu 9216
```

Questa configurazione garantisce che l'MTU del jumbo frame L2 supportata dai moduli sia sempre inferiore o uguale al valore configurato per le interfacce L3 attraversate dal traffico. Ciò impedisce la frammentazione quando il traffico viene instradato dalla VLAN sull'interfaccia L3.

Configurazione gestione

In questa sezione vengono illustrate alcune considerazioni relative al controllo, al provisioning e alla risoluzione dei problemi di una rete Catalyst.

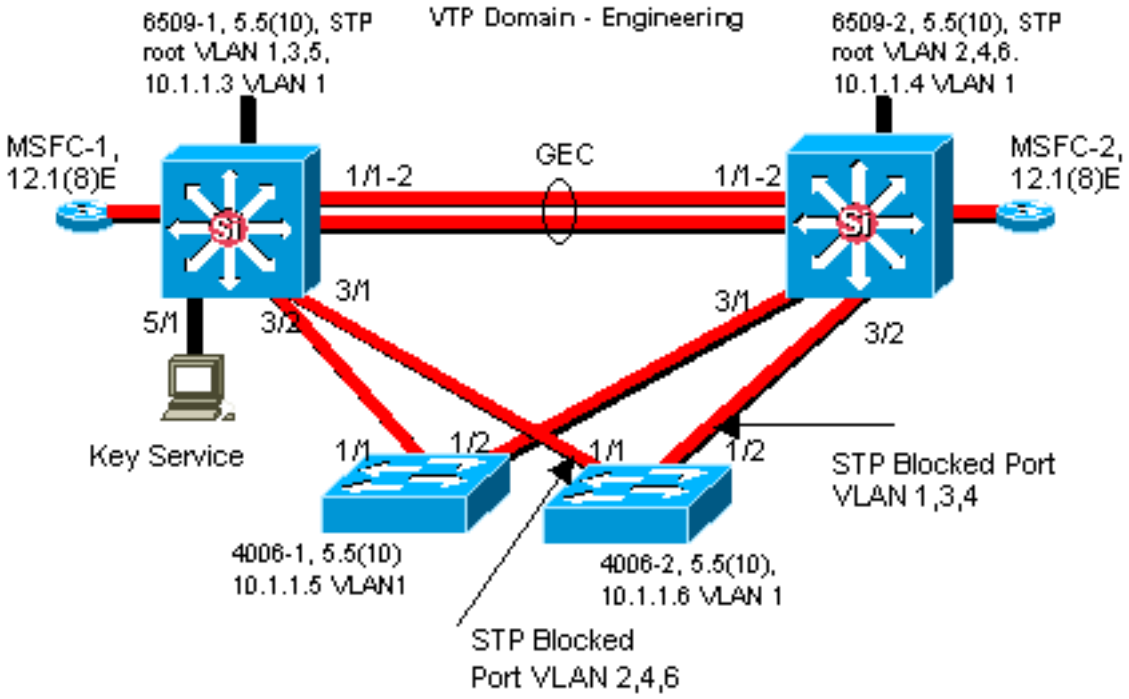
Diagrammi di rete

I chiari diagrammi di rete sono una parte fondamentale delle operazioni di rete. Diventano fondamentali durante la risoluzione dei problemi e sono il veicolo più importante per la comunicazione delle informazioni quando vengono inoltrate a fornitori e partner durante un'interruzione delle attività. La loro preparazione, prontezza e accessibilità non devono essere sottovalutate.

Suggerimento

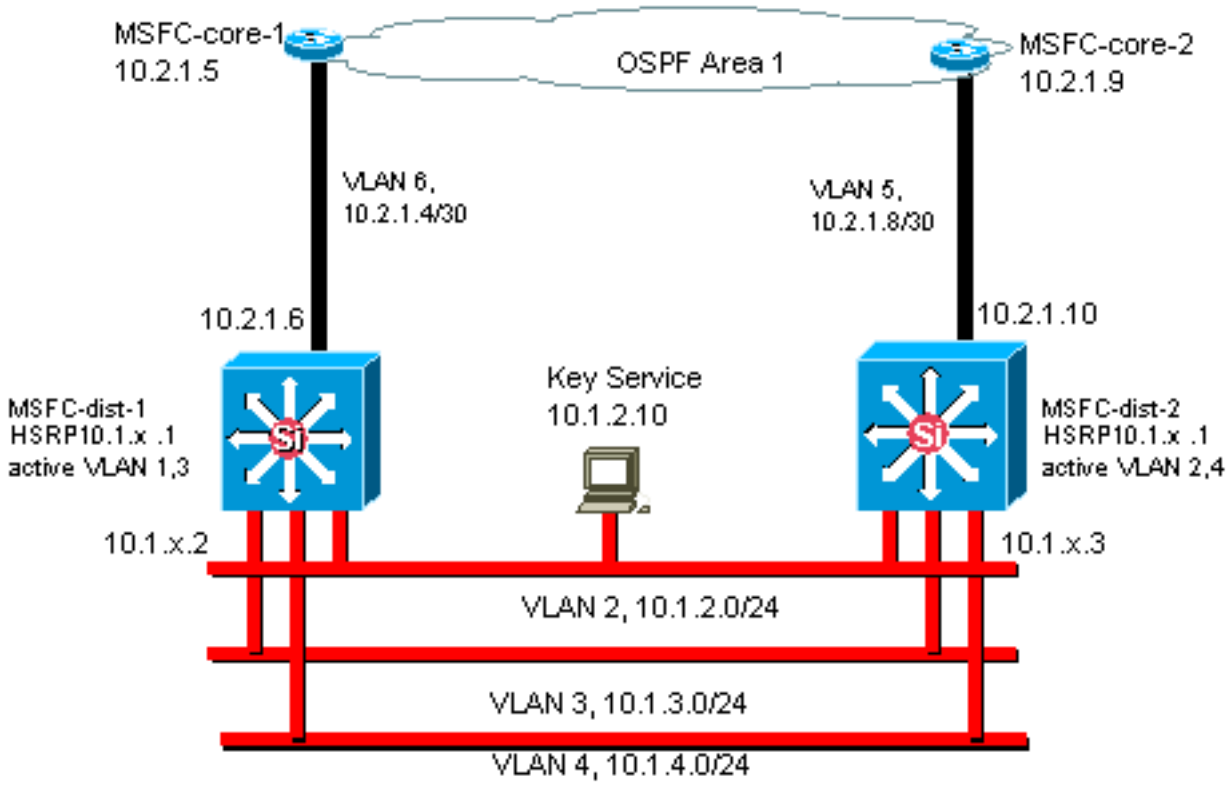
Cisco consiglia di creare i seguenti tre diagrammi:

- **Diagramma generale**: anche per le reti più grandi è importante disporre di un diagramma che indichi la connettività fisica e logica end-to-end. Può essere comune per le aziende che hanno implementato una struttura gerarchica documentare ogni livello separatamente. Durante la pianificazione e la risoluzione dei problemi, tuttavia, è spesso una buona conoscenza di come i domini collegano tra loro che conta.
- **Physical Diagram**: visualizza tutti i componenti hardware e i cavi dello switch e del router. È necessario etichettare trunk, collegamenti, velocità, gruppi di canali, numeri di porta, slot, tipi di chassis, software, domini VTP, root bridge, priorità del root bridge di backup, indirizzo MAC e porte bloccate per VLAN. Spesso è più chiaro rappresentare i dispositivi interni, ad esempio l'MSFC Catalyst 6500/6000, come router su uno stick collegato tramite un



trunk.

- **Diagramma logico**: mostra solo la funzionalità L3 (router come oggetti, VLAN come segmenti Ethernet). È necessario etichettare gli indirizzi IP, le subnet, l'indirizzamento secondario, l'HSRP attivo e in standby, i livelli di distribuzione dei core di accesso e le informazioni di routing.



Gestione In-Band

A seconda della configurazione, l'interfaccia di gestione in banda (interna) dello switch (nota come sc0) potrebbe dover gestire questi dati:

- Protocolli di gestione dello switch, ad esempio SNMP, Telnet, SSH (Secure Shell Protocol) e syslog

- Dati utente quali broadcast e multicast
- Protocolli di controllo dello switch, ad esempio BPDU STP, VTP, DTP, CDP, ecc.

Nella progettazione multilayer di Cisco, è pratica comune configurare una VLAN di gestione che si estenda su un dominio commutato e contenga tutte le interfacce sc0. Ciò aiuta a separare il traffico di gestione dal traffico degli utenti e aumenta la sicurezza delle interfacce di gestione dello switch. In questa sezione vengono descritti il significato e i potenziali problemi dell'uso della VLAN predefinita 1 e dell'esecuzione del traffico di gestione sullo switch nella stessa VLAN del traffico utente.

Panoramica operativa

La preoccupazione principale sull'uso della VLAN 1 per i dati utente è che il protocollo NMP del Supervisor Engine in generale non deve essere interrotto da gran parte del traffico multicast e broadcast generato dalle stazioni terminali. L'hardware Catalyst 5500/5000 precedente, in particolare Supervisor Engine I e Supervisor Engine II, dispone di risorse limitate per la gestione di questo traffico, anche se il principio si applica a tutti i Supervisor Engine. Se la CPU del Supervisor Engine, il buffer o il canale in-band del backplane sono occupati in modo completo durante l'ascolto di traffico non necessario, è possibile che i frame di controllo non vengano visualizzati. Nello scenario peggiore, questa condizione potrebbe causare un loop nello Spanning Tree o un errore di EtherChannel.

Se i comandi show interface e **show ip status** vengono emessi sul Catalyst, possono fornire un'indicazione della proporzione del traffico broadcast sul traffico unicast e della proporzione del traffico IP sul traffico non IP (in genere non presente nelle VLAN di gestione).

Un ulteriore controllo dello stato dei vecchi dispositivi hardware Catalyst 5500/5000 consiste nell'esaminare i risultati del comando **show** ***inband*** | *biga* (comando nascosto) per errori di risorse (RscrcErrors), simile alle perdite di buffer in un router. Se gli errori delle risorse aumentano continuamente, la memoria non è disponibile per ricevere i pacchetti di sistema, probabilmente a causa di una quantità significativa di traffico broadcast nella VLAN di gestione. Un errore relativo a una singola risorsa può significare che il Supervisor Engine non è in grado di elaborare un pacchetto, ad esempio BPDU, e questo potrebbe rapidamente diventare un problema perché i protocolli come lo Spanning Tree non inviano nuovamente i BPDU mancanti.

Suggerimento

Come evidenziato nella sezione Controllo Cat di questo documento, la VLAN 1 è una VLAN speciale che applica tag e gestisce la maggior parte del traffico del control plane. La VLAN 1 è abilitata su tutti i trunk per impostazione predefinita. Con reti di campus più grandi, è necessario prestare attenzione al diametro del **dominio** VLAN 1 **STP**; l'instabilità di una parte della rete potrebbe influire sulla VLAN 1, influendo quindi sulla stabilità del control plane e sulla stabilità dell'STP di tutte le altre VLAN. In CatOS 5.4 e versioni successive, è stato possibile impedire alla VLAN 1 di trasportare i dati dell'utente ed eseguire STP con questo comando:

```
clear trunk mod/port vlan 1
```

Ciò non impedisce che i pacchetti di controllo vengano inviati da uno switch all'altro nella VLAN 1, come mostrato con un analizzatore di rete. Tuttavia, non viene inoltrato alcun dato e STP non viene eseguito su questo collegamento. Pertanto, questa tecnica può essere utilizzata per suddividere la VLAN 1 in domini di errore più piccoli.

Nota: Al momento non è possibile cancellare i trunk della VLAN 1 sugli switch 3500 e 2900XL.

Anche se si è prestata attenzione alla progettazione del campus per vincolare le VLAN utente a domini di switch relativamente piccoli e di conseguenza a piccoli errori/limiti L3, alcuni clienti sono ancora tentati di trattare la VLAN di gestione in modo diverso e cercare di coprire l'intera rete con una singola subnet di gestione. Non vi è alcun motivo tecnico per cui un'applicazione NMS centrale debba essere adiacente ai dispositivi che gestisce, né si tratta di un argomento di sicurezza qualificato. Cisco consiglia di limitare il diametro delle VLAN di gestione alla stessa struttura di dominio routing delle VLAN utente e di considerare la gestione fuori banda e/o il supporto SSH CatOS 6.x come un modo per aumentare la sicurezza della gestione della rete.

Altre opzioni

Tuttavia, per queste raccomandazioni Cisco, per alcune topologie sono necessarie considerazioni di progettazione. Ad esempio, un progetto multilayer Cisco comune e desiderabile evita l'uso di uno Spanning Tree attivo. È quindi necessario vincolare ciascuna subnet IP/VLAN a un singolo switch di livello di accesso o a un cluster di switch. In questi progetti, non potrebbe esistere alcun trunking configurato fino al livello di accesso.

Non c'è una risposta semplice alla domanda se creare una VLAN di gestione separata e abilitare il trunking per trasportarla tra i livelli di accesso L2 e distribuzione L3. Di seguito sono riportate due opzioni per la revisione del progetto con il tecnico Cisco:

- **Opzione 1:** collegare due o tre VLAN univoche dal livello di distribuzione a ciascuno switch del livello di accesso. Ciò consente, ad esempio, una VLAN dati, una VLAN voce e una VLAN di gestione e ha ancora il vantaggio che l'STP non è attivo. (notare che se la VLAN 1 viene eliminata dai trunk, è presente un passaggio di configurazione aggiuntivo.) In questa soluzione, è necessario considerare anche i punti di progettazione per evitare il blocco temporaneo del traffico indirizzato durante il ripristino in caso di errore: Stp PortFast per trunk (CatOS 7.x e versioni successive) o sincronizzazione automatica VLAN con inoltro STP (versioni successive a CatOS 5.5[9]).
- **Opzione 2:** una singola VLAN per i dati e la gestione potrebbe essere accettabile. Con hardware di switching più recente, come CPU più potenti e controlli per la limitazione della velocità del control plane, più un design con domini di broadcast relativamente piccoli come richiesto dal design multilivello, per molti clienti la separazione dell'interfaccia sc0 dai dati dell'utente è meno problematica di una volta. Per prendere una decisione finale, occorre probabilmente esaminare il profilo del traffico di broadcast della VLAN e discutere con il tecnico Cisco le funzionalità dell'hardware dello switch. Se la VLAN di gestione contiene effettivamente tutti gli utenti su tale switch del livello di accesso, si consiglia di utilizzare filtri di input IP per proteggere lo switch dagli utenti, come indicato nella sezione Configurazione della sicurezza in questo documento.

Gestione fuori banda

Sulla base delle argomentazioni della sezione precedente, la gestione della rete può essere resa più disponibile con la costruzione di un'infrastruttura di gestione separata intorno alla rete di produzione, in modo che i dispositivi siano sempre raggiungibili in remoto indipendentemente dagli eventi del traffic-driven o del control-plane. Questi due approcci sono tipici:

- Gestione fuori banda con una LAN esclusiva

- Gestione fuori banda con server terminal

Panoramica operativa

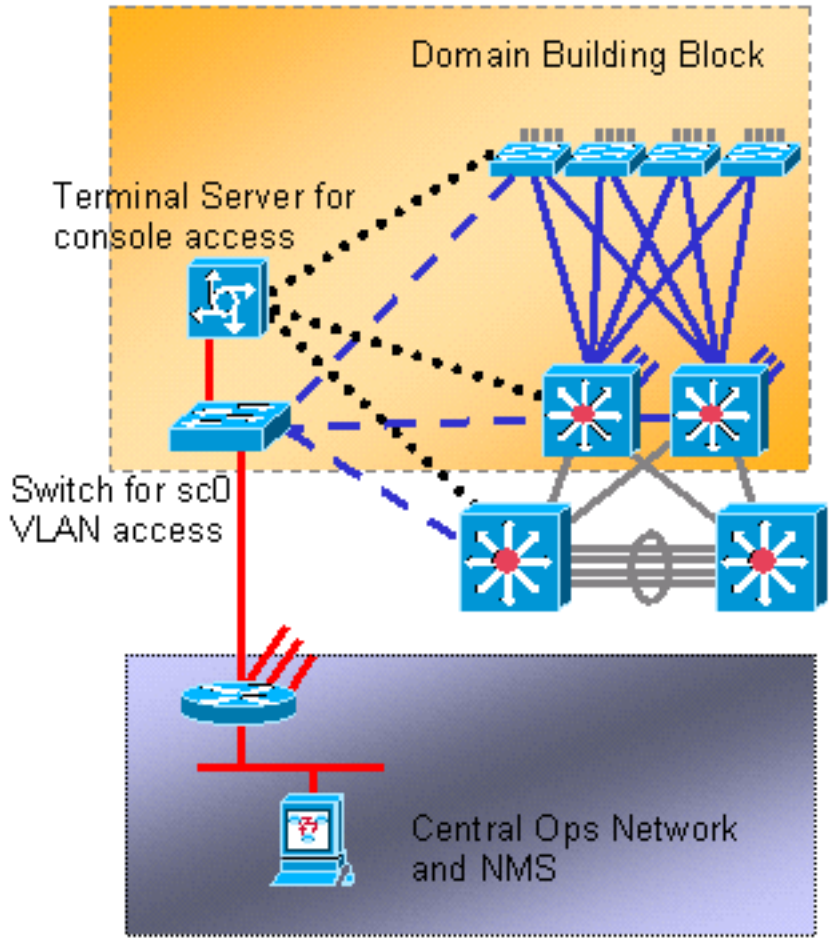
Su una VLAN di gestione, ogni router e switch della rete possono essere forniti con un'interfaccia di gestione Ethernet fuori banda. Una porta Ethernet su ciascun dispositivo è configurata nella VLAN di gestione e cablata all'esterno della rete di produzione su una rete di gestione commutata separata tramite l'interfaccia sc0. Notare che gli switch Catalyst 4500/4000 dispongono di un'interfaccia me1 speciale sul Supervisor Engine che deve essere utilizzata solo per la gestione fuori banda, non come porta dello switch.

Inoltre, la connettività del server terminal può essere ottenuta tramite una configurazione Cisco 2600 o 3600 con cavi da RJ-45 a seriale per accedere alla porta console di ogni router e switch del layout. Un server terminal evita inoltre la necessità di configurare scenari di backup, ad esempio modem su porte ausiliarie per ogni dispositivo. È possibile configurare un singolo modem sulla porta ausiliaria del Terminal Server per fornire il servizio di connessione remota agli altri dispositivi durante un errore di connettività di rete.

Suggerimento

Con questa disposizione, sono possibili due percorsi fuori banda per ogni switch e router, oltre a numerosi percorsi in-band, consentendo in tal modo una gestione di rete ad alta disponibilità. Fuori banda è responsabile di:

- Il traffico di gestione è separato fuori banda dai dati utente.
- L'indirizzo IP di gestione è contenuto in una subnet, una VLAN e uno switch separati per una maggiore sicurezza.
- La modalità fuori banda garantisce una maggiore sicurezza nella distribuzione dei dati di gestione durante gli errori di rete.
- Lo Spanning Tree non è attivo nella VLAN di gestione per la modalità fuori banda. La ridondanza non è un fattore critico.



Test di sistema

Diagnostica di avvio

Durante l'avvio del sistema, vengono eseguiti diversi processi per garantire la disponibilità di una piattaforma affidabile e operativa, in modo che l'hardware difettoso non interferisca con la rete. La diagnostica di avvio di Catalyst è suddivisa tra POST (Power-On Self Test) e diagnostica online.

Panoramica operativa

A seconda della configurazione della piattaforma e dell'hardware, all'avvio e quando una scheda viene sostituita a caldo nello chassis vengono eseguite diverse operazioni di diagnostica. Un livello di diagnostica più elevato determina un numero maggiore di problemi rilevati, ma un ciclo di avvio più lungo. È possibile selezionare tre livelli di diagnostica POST (tutti i test verificano la presenza e le dimensioni di DRAM, RAM e cache e li inizializzano):

Panoramica operativa			
Ignora	N/D	3	Non disponibile nella serie 4500/4000 con CatOS 5.5 o versioni precedenti.
Minima	I test di scrittura dei modelli vengono eseguiti solo sui primi MB di DRAM.	30	predefinito sulle serie 5500/5000 e 6500/6000; non disponibile nella serie

			4500/4000.
Completa	Test di scrittura dei modelli per tutta la memoria.	60	Impostazione predefinita sulla serie 4500/4000.

Diagnostica online

Questi test verificano i percorsi dei pacchetti internamente allo switch. È importante notare che la diagnostica online è pertanto un test a livello di sistema e non semplicemente un test delle porte. Sugli switch Catalyst 5500/5000 e 6500/6000, i test vengono eseguiti prima dal Supervisor Engine di standby, quindi nuovamente dal Supervisor Engine principale. La lunghezza della diagnostica dipende dalla configurazione del sistema (numero di slot, moduli, porte). Esistono tre categorie di test:

- Test di loopback: i pacchetti provenienti dal Supervisor Engine NMP vengono inviati a ciascuna porta, quindi vengono restituiti al NMP e analizzati per rilevare eventuali errori.
- Test di bundling: vengono creati canali con un massimo di otto porte e vengono eseguiti test di loopback alla porta agport per verificare l'hashing a collegamenti specifici (per ulteriori informazioni, fare riferimento alla sezione EtherChannel di questo documento).
- Test Enhanced Address Recognition Logic (EARL): vengono testati sia il Supervisor Engine centrale che i motori di riscrittura L3 del modulo Ethernet in linea. Le voci di inoltro hardware e le porte indirizzate vengono create prima dell'invio di pacchetti di esempio (per ciascun tipo di incapsulamento del protocollo) dal protocollo di rete tramite l'hardware di commutazione su ciascun modulo e di nuovo al protocollo di rete. Questa procedura è valida per i moduli Catalyst 6500/6000 PFC e versioni successive.

La diagnostica online completa può richiedere circa due minuti. La diagnostica minima non esegue il test bundle o rewrite su moduli diversi dal Supervisor Engine e può richiedere circa 90 secondi.

Durante un test di memoria, quando viene rilevata una differenza nella lettura dello schema rispetto allo schema scritto, lo stato della porta viene modificato in `faulty`. I risultati di questi test possono essere visualizzati se si usa il comando **show test**, seguito dal numero del modulo da esaminare:

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ---------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ---------------- . . . .
```

Suggerimento

Cisco consiglia di impostare tutti gli switch in modo da utilizzare la diagnostica completa per fornire il massimo rilevamento degli errori e prevenire interruzioni durante le normali operazioni.

Nota: questa modifica sarà effettiva al prossimo avvio del dispositivo. Per impostare la diagnostica completa, usare questo comando:

```
set test diaglevel complete
```

Altre opzioni

In alcune situazioni, un tempo di avvio rapido può essere preferibile rispetto all'attesa di eseguire la diagnostica completa. Ci sono altri fattori e tempi coinvolti nel sollevare un sistema, ma nel complesso, POST e diagnostica online aggiungono circa un terzo di nuovo nel tempo. Nei test eseguiti con uno chassis a nove slot Supervisor Engine singolo completamente popolato con Catalyst 6509, il tempo di avvio totale è stato di circa 380 secondi con diagnostica completa, circa 300 secondi con diagnostica minima e solo 250 secondi con diagnostica ignorata. Utilizzare questo comando per configurare il bypass:

```
set test diaglevel bypass
```

Nota: Catalyst 4500/4000 accetta di essere configurato per una diagnostica minima, ma questa operazione determina comunque l'esecuzione di un test completo. La modalità minima potrebbe essere supportata in futuro su questa piattaforma.

Diagnostica tempo di esecuzione

Una volta operativo il sistema, il Supervisor Engine dello switch esegue vari monitoraggi sugli altri moduli. Se un modulo non è raggiungibile tramite i messaggi di gestione (Serial Control Protocol [SCP] in esecuzione sul bus di gestione fuori banda), il Supervisor Engine tenta di riavviare la scheda o di adottare altre misure appropriate.

Panoramica operativa

Il Supervisor Engine effettua automaticamente vari controlli; non è necessaria alcuna configurazione. Sugli switch Catalyst 5500/5000 e 6500/6000, vengono monitorati questi componenti dello switch:

- NMP attraverso un watchdog
- Errori avanzati del chip EARL
- Canale in banda dal Supervisor Engine al backplane
- Moduli tramite keepalive su canale fuori banda (Catalyst 6500/6000)
- Il Supervisor Engine attivo viene monitorato dal Supervisor Engine di standby per determinarne lo stato (Catalyst 6500/6000)

Rilevamento errori di sistema e hardware

Panoramica operativa

In CatOS 6.2 e versioni successive, sono state aggiunte ulteriori funzionalità per il monitoraggio dei componenti critici a livello di sistema e hardware. Sono supportati i seguenti tre componenti hardware:

- In banda

- Contatore porte
- Memoria

Quando la funzione è abilitata e viene rilevata una condizione di errore, lo switch genera un messaggio syslog. Il messaggio informa l'amministratore che esiste un problema prima che si verifichi un calo notevole delle prestazioni. Nelle versioni CatOS 6.4(16), 7.6(12), 8.4(2) e successive, la modalità predefinita per tutti e tre i componenti è stata modificata da disabilitata a abilitata.

In banda

Se viene rilevato un errore in banda, un messaggio syslog informa che esiste un problema prima che si verifichi un notevole calo delle prestazioni. L'errore indica il tipo di errore in banda. Alcuni esempi sono:

- Inband bloccato
- Errori delle risorse
- Errore in banda durante l'avvio

Quando viene rilevato un errore di ping in banda, la funzione restituisce un messaggio syslog aggiuntivo con un'istantanea della velocità Tx e Rx corrente sulla connessione in banda, sulla CPU e sul carico del backplane dello switch. Questo messaggio consente di determinare correttamente se il segnale in banda è bloccato (senza Tx/Rx) o sovraccarico (Tx/Rx eccessivo). Queste informazioni aggiuntive possono aiutare a determinare la causa degli errori di ping in banda.

Contatore porte

Quando si attiva questa funzionalità, viene creato e avviato un processo per il debug dei contatori delle porte. Il contatore delle porte controlla periodicamente alcuni contatori di errori delle porte interne. L'architettura della scheda di linea, in particolare gli ASIC del modulo, determina i contatori su cui le funzionalità vengono interrogate. Il supporto tecnico Cisco o i tecnici di sviluppo possono quindi utilizzare queste informazioni per risolvere i problemi. Questa funzionalità non esegue il polling dei contatori di errori, ad esempio FCS, CRC, alignment e runt, direttamente associati alla connettività del partner di collegamento. Per incorporare questa funzionalità, vedere la sezione Gestione degli errori di EtherChannel/Link di questo documento.

Il polling viene eseguito ogni 30 minuti e viene eseguito in background nei contatori di errori selezionati. Se il conteggio aumenta tra due polling successivi sulla stessa porta, un messaggio syslog segnala l'incidente e fornisce il modulo/porta e i dettagli del contatore degli errori.

L'opzione del contatore della porta non è supportata sulla piattaforma Catalyst 4500/4000.

Memoria

L'attivazione di questa funzione consente di eseguire il monitoraggio in background e di rilevare le condizioni di danneggiamento della DRAM. Tali condizioni di danneggiamento della memoria includono:

- Allocazione
- Liberazione
- Fuori intervallo

- Allineamento non valido

Suggerimento

Abilitare tutte le funzionalità di rilevamento degli errori, inclusi i contatori in banda, delle porte e della memoria, dove sono supportati. L'abilitazione di queste funzionalità migliora la diagnostica proattiva degli avvisi di sistema e hardware per la piattaforma dello switch Catalyst. Utilizzare questi comandi per abilitare tutte e tre le funzionalità di rilevamento degli errori:

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Per verificare che il rilevamento errori sia abilitato, usare questo comando:

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

Gestione degli errori EtherChannel/Link

Panoramica operativa

In CatOS 8.4 e versioni successive, è stata introdotta una nuova funzionalità per fornire un failover automatico del traffico da una porta di EtherChannel a un'altra porta dello stesso EtherChannel. Il failover delle porte si verifica quando una delle porte nel canale supera una soglia di errore configurabile entro l'intervallo specificato. Il failover della porta si verifica solo se in EtherChannel è presente una porta operativa. Se la porta in errore è l'ultima porta di EtherChannel, la porta non entra nello stato `port-failover`. Questa porta continua a trasmettere il traffico, indipendentemente dal tipo di errori ricevuti. Le porte singole non raggruppate in un canale non passano allo stato `port-failover`. Lo stato err-disabled viene generato per queste porte quando la soglia di errore viene superata nell'intervallo specificato.

Questa funzione è efficace solo quando si abilitano i **contatori di porta set errordetection**. Gli errori di collegamento da monitorare si basano su tre contatori:

- InErrori
- RxCRC (CRCAlignErrors)
- TxCRC

Per visualizzare il numero di contatori di errore, usare il comando **show counters** su uno switch. Questo è un esempio:

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

Questa tabella contiene una lista dei possibili parametri di configurazione e la relativa configurazione di default:

Parametri	Predefinito
Globale	Disattivato
Monitor porta per RxCRC	Disattivato
Monitor porta per InErrors	Disattivato
Monitor porta per TxCRC	Disattivato
Azione	Failover delle porte
Intervallo	30 secondi
Conteggio campionamento	3 consecutivi
Soglia bassa	1000
Soglia alta	1001

Se la funzione è abilitata e il numero di errori di una porta raggiunge il valore massimo della soglia configurabile entro il periodo di conteggio di campionamento specificato, l'azione configurabile è la disabilitazione degli errori o il failover delle porte. L'azione error disable porta allo stato `err-disabled`. Se si configura l'azione di failover della porta, viene preso in considerazione lo stato del canale della porta. La porta viene disabilitata a causa di un errore solo se è collegata a un canale, ma non è l'ultima porta operativa del canale. Inoltre, se l'azione configurata è il failover della porta e la porta è una porta singola o non canalizzata, la porta viene messa nello stato `err-disabled` quando il numero di errori della porta raggiunge il valore massimo della soglia.

L'intervallo è una costante del timer per la lettura dei contatori degli errori della porta. Il valore predefinito dell'intervallo degli errori di collegamento è 30 secondi. L'intervallo consentito è compreso tra 30 e 1800 secondi.

Esiste il rischio di disabilitazione accidentale di una porta a causa di un evento singolo imprevisto. Per ridurre al minimo questo rischio, le azioni da eseguire su una porta vengono eseguite solo quando la condizione persiste per il numero di volte specificato nel campionamento consecutivo. Il valore di campionamento predefinito è 3 e l'intervallo consentito è compreso tra 1 e 255.

La soglia è un numero assoluto da controllare in base all'intervallo degli errori di collegamento. La soglia minima di errore di collegamento predefinita è 1000 e l'intervallo consentito è compreso tra 1 e 65.535. La soglia massima di errore di collegamento predefinita è 1001. Quando il numero consecutivo di campionamenti raggiunge la soglia bassa, viene inviato un syslog. Se i tempi di campionamento consecutivi raggiungono la soglia massima, viene inviato un syslog e viene attivata un'azione di disabilitazione dell'errore o di failover della porta.

Nota: utilizzare la stessa configurazione di rilevamento errori porte per tutte le porte di un canale. Per ulteriori informazioni, consultare le seguenti sezioni della guida alla configurazione del software Catalyst serie 6500:

- Sezione *Configurazione della gestione degli errori EtherChannel/Link* in Controllo dello stato e della connettività
- Sezione *Configurazione del rilevamento degli errori delle porte* in Configurazione di Ethernet, Fast Ethernet, Gigabit Ethernet e switching Ethernet da 10 Gigabit

Raccomandazioni

Poiché la funzionalità utilizza messaggi SCP per registrare e confrontare i dati, un numero elevato di porte attive può richiedere un utilizzo intensivo della CPU. Questo scenario richiede un utilizzo ancora più intensivo della CPU quando l'intervallo di soglia è impostato su un valore molto basso. Abilitare questa funzione con discrezione per le porte designate come collegamenti critici e che trasportano il traffico per le applicazioni sensibili. Per abilitare il rilevamento globale degli errori dei collegamenti, eseguire questo comando:

```
set errordetection link-errors enable
```

Inoltre, iniziate con i parametri di soglia, intervallo e campionamento predefiniti. Utilizzare l'azione predefinita failover delle porte.

Per applicare i parametri degli errori di collegamento globali a singole porte, eseguire questi comandi:

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

Èpossibile utilizzare questi comandi per verificare la configurazione degli errori di collegamento:

```
show errordetection

show port errordetection {mod | mod/port}
```

Diagnostica buffer di pacchetto Catalyst 6500/6000

Nelle versioni CatOS 6.4(7), 7.6(5) e 8.2(1), è stata introdotta la diagnostica dei buffer di pacchetto Catalyst 6500/6000. La diagnostica del buffer di pacchetto, abilitata per impostazione predefinita, rileva gli errori del buffer di pacchetto causati da errori temporanei della RAM statica (SRAM). Il rilevamento viene eseguito sui seguenti moduli di linea 10/100-Mbps a 48 porte:

- WS-X6248-RJ45
- WS-X6248-RJ21

- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

In caso di guasto, 12 delle 48 porte a 10/100 Mbps continuano a rimanere connesse e possono verificarsi problemi di connettività casuale. L'unico modo per riprendersi da questa condizione è spegnere e riaccendere il modulo di linea.

Panoramica operativa

La diagnostica del buffer di pacchetto controlla i dati archiviati in una sezione specifica del buffer di pacchetto per determinare se è danneggiato da errori SRAM temporanei. Se il processo legge qualcosa di diverso da quello scritto, esegue due possibili opzioni di ripristino configurabili:

1. Per impostazione predefinita, le porte della scheda di linea interessate dall'errore del buffer vengono disabilitate.
2. La seconda opzione consiste nel spegnere e riaccendere la scheda di linea.

Sono stati aggiunti due messaggi syslog. I messaggi forniscono un avviso relativo alla disabilitazione delle porte o al ciclo di alimentazione del modulo a causa di errori del buffer del pacchetto:

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

Nelle versioni CatOS precedenti alla 8.3 e 8.4, la durata del ciclo di alimentazione della scheda di linea è compresa tra 30 e 40 secondi. Nelle versioni 8.3 e 8.4 di CatOS è stata introdotta una funzione di avvio rapido, che scarica automaticamente il firmware sulle schede di linea installate durante il processo di avvio iniziale per ridurre al minimo il tempo di avvio. La funzione di avvio rapido riduce il tempo di ciclo di alimentazione a circa 10 secondi.

Suggerimento

Cisco consiglia di *disabilitare* l'opzione predefinita. Questa azione ha il minore impatto sul servizio di rete durante le ore di produzione. Se possibile, per ripristinare il servizio, spostare la connessione interessata dalle porte disabilitate a causa di un errore su altre porte dello switch disponibili. Programmare un ciclo di alimentazione manuale della scheda di linea durante la finestra di manutenzione. Usare il comando reset module *mod* per ripristinare completamente la condizione del buffer del pacchetto danneggiato.

Nota: se gli errori continuano dopo la reimpostazione del modulo, provare a riposizionare il modulo.

Per abilitare l'opzione *errdisable*, usare questo comando:

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Altra opzione

Poiché è necessario un ciclo di alimentazione della scheda di linea per ripristinare completamente tutte le porte in cui si è verificato un errore SRAM, un'azione di ripristino alternativa consiste nella configurazione dell'opzione del ciclo di alimentazione. Questa opzione è utile quando è accettabile un'interruzione nei servizi di rete che può durare da 30 a 40 secondi. Questo periodo di tempo è il tempo necessario a un modulo di linea per spegnere e riaccendere completamente il sistema e rimettersi in servizio senza la funzione di avvio rapido. La funzione di avvio rapido consente di ridurre a 10 secondi il tempo di interruzione dei servizi di rete con l'opzione del ciclo di alimentazione. Per abilitare l'opzione del ciclo di alimentazione, usare questo comando:

```
set errordetection packet-buffer power-cycle
```

Diagnostica buffer di pacchetto

Questo test è valido solo sugli switch Catalyst 5500/5000. Questo test è progettato per rilevare eventuali guasti hardware sugli switch Catalyst 5500/5000 che utilizzano moduli Ethernet con hardware specifico che fornisce una connettività a 10/100 Mbps tra le porte utente e il backplane dello switch. Poiché non possono eseguire il controllo CRC dei frame trunking, se un buffer del pacchetto della porta diventa difettoso durante il runtime, i pacchetti potrebbero danneggiarsi e causare errori CRC. Sfortunatamente, ciò potrebbe portare alla propagazione di frame danneggiati ulteriormente nella rete Catalyst 5500/5000 ISL, il che potrebbe causare problemi al control plane e tempeste broadcast negli scenari peggiori.

I moduli Catalyst 5500/5000 più recenti e altre piattaforme hanno aggiornato il controllo degli errori hardware integrato e non richiedono i test del buffer dei pacchetti, quindi non è possibile configurarlo.

I moduli di linea che necessitano della diagnostica del buffer dei pacchetti sono WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5201, WS-X5203, WS-X5213/a, WS-X5223 5224, WS-X5506, WS-X5509, WS-U5531, WS-U5533 e WS-U5535.

Panoramica operativa

Questa diagnostica controlla che i dati memorizzati in una sezione specifica del buffer del pacchetto non vengano danneggiati accidentalmente da hardware difettoso. Se il processo rilegge qualcosa di diverso da quello scritto, la porta viene chiusa in modalità `non riuscita`, poiché potrebbe danneggiare i dati. Non è necessaria alcuna soglia di errore. Le porte con errori non possono essere riattivate finché il modulo non viene reimpostato o sostituito.

I test del buffer di pacchetto possono essere eseguiti in due modalità: programmate e su richiesta. Quando inizia un test, vengono generati messaggi syslog per indicare la lunghezza prevista del test (arrotondata al minuto più vicino) e il fatto che il test è stato avviato. La lunghezza esatta del test varia in base al tipo di porta, alle dimensioni del buffer e al tipo di esecuzione dei test.

I test on demand sono molto impegnativi e possono essere completati in pochi minuti. Poiché questi test interferiscono attivamente con la memoria del pacchetto, le porte devono essere chiuse a livello amministrativo prima del test. Per arrestare le porte, usare questo comando:

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
```

```
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

I test pianificati sono molto meno aggressivi dei test su richiesta e vengono eseguiti in background. I test vengono eseguiti in parallelo su più moduli, ma su una porta per modulo alla volta. Il test conserva, scrive e legge piccole sezioni della memoria buffer del pacchetto prima di ripristinare i dati del buffer del pacchetto dell'utente, e quindi non genera errori. Tuttavia, poiché il test viene scritto nella memoria buffer, blocca i pacchetti in arrivo per alcuni millisecondi e causa una perdita sui collegamenti occupati. Per impostazione predefinita, tra un test di scrittura del buffer e l'altro si verifica una pausa di otto secondi per ridurre al minimo la perdita dei pacchetti, ma questo significa che un sistema pieno di moduli che necessitano di un test del buffer del pacchetto può impiegare più di 24 ore per completare il test. Per impostazione predefinita, questo test pianificato viene eseguito ogni settimana alle 03.30 della domenica da CatOS 5.4 o versioni successive e lo stato del test può essere confermato con questo comando:

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Suggerimento

Cisco consiglia di utilizzare la funzionalità di test pianificato del buffer di pacchetto per i sistemi Catalyst 5500/5000, in quanto il vantaggio di rilevare i problemi sui moduli supera il rischio di una bassa perdita di pacchetti.

Èquindi necessario pianificare un orario settimanale standardizzato sulla rete che consenta al cliente di modificare i collegamenti dalle porte difettose o dai moduli RMA, se necessario. Poiché questo test può causare la perdita di alcuni pacchetti, a seconda del carico di rete, è necessario programmare orari di rete più tranquilli, ad esempio l'impostazione predefinita delle 3.30 di domenica mattina. Utilizzare questo comando per impostare l'ora del test:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Una volta abilitato (come quando CatOS viene aggiornato alla versione 5.4 e successive per la prima volta), esiste la possibilità che un problema di memoria/hardware precedentemente nascosto sia esposto e che una porta venga chiusa automaticamente di conseguenza. È possibile visualizzare questo messaggio:

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

Altre opzioni

Se non è accettabile il rischio di una bassa perdita di pacchetti per porta su base settimanale, si consiglia di utilizzare la funzione su richiesta durante le interruzioni pianificate. Per avviare manualmente questa funzione per ciascun intervallo, eseguire questo comando (anche se la porta deve essere prima disabilitata a livello amministrativo):

```
test packetbuffer port range
```

Log di sistema

I messaggi Syslog sono specifici di Cisco e sono fondamentali per la gestione proattiva degli errori. Utilizzando syslog viene segnalata una gamma più ampia di condizioni di rete e di protocollo rispetto a quella possibile con il protocollo SNMP standardizzato. Le piattaforme di gestione, ad esempio Cisco Resource Manager Essentials (RME) e Network Analysis Toolkit (NATkit), utilizzano in modo efficace le informazioni di syslog in quanto eseguono le seguenti attività:

- Presentazione dell'analisi per gravità, messaggio, dispositivo e così via
- Abilita il filtro dei messaggi in arrivo per l'analisi
- Attivazione di avvisi, ad esempio cercapersone, o raccolta su richiesta delle modifiche alle scorte e alla configurazione

Suggerimento

Un punto importante su cui focalizzare l'attenzione è il livello delle informazioni di log che devono essere generate localmente e conservate nel buffer dello switch, a differenza di quanto viene inviato a un server syslog (usando il comando set logging server severity *value*). Alcune organizzazioni registrano un livello elevato di informazioni a livello centrale, mentre altre accedono allo switch stesso per esaminare i registri più dettagliati di un evento o per abilitare un livello più elevato di acquisizione del syslog solo durante la risoluzione dei problemi.

Il debug è diverso sulle piattaforme CatOS dal software Cisco IOS, ma la registrazione dettagliata del sistema può essere abilitata per singola sessione con l'impostazione della sessione di registrazione abilitata senza modificare l'elemento registrato per impostazione predefinita.

Cisco in genere consiglia di portare le funzionalità di syslog di spantree e di sistema al livello 6, in quanto si tratta delle caratteristiche chiave di stabilità da tenere traccia. Inoltre, per gli ambienti multicast, si consiglia di portare il livello di registrazione della funzione mcast a 4, in modo da generare messaggi syslog in caso di eliminazione delle porte del router. Sfortunatamente, prima di CatOS 5.5(5) questo potrebbe causare la registrazione di messaggi syslog per join e foglie IGMP, che è troppo rumoroso da monitorare. Infine, se si usano elenchi di input IP, si consiglia un livello di registrazione minimo di 4 per acquisire i tentativi di accesso non autorizzati. Utilizzare questi comandi per impostare le seguenti opzioni:

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Spegnere i messaggi della console per evitare che lo switch si blocchi in attesa di una risposta da un terminale lento o inesistente quando il volume dei messaggi è elevato. La registrazione della

console è una priorità elevata in CatOS e viene utilizzata principalmente per acquisire i messaggi finali localmente in caso di risoluzione dei problemi o di arresto anomalo dello switch.

In questa tabella vengono fornite le singole funzionalità di log, i livelli predefiniti e le modifiche consigliate per Catalyst 6500/6000. Ogni piattaforma dispone di funzionalità leggermente diverse, a seconda delle funzionalità supportate.

Struttura	Livello predefinito	Azione consigliata
acl	5	Lasciate stare.
cdp	4	Lasciate stare.
poliziotti	3	Lasciate stare.
dtp	8	Lasciate stare.
conte	2	Lasciate stare.
etica[1]	5	Lasciate stare.
filesys	2	Lasciate stare.
gvrp	2	Lasciate stare.
ip	2	Se si usano elenchi di input IP, passare a 4.
kernel	2	Lasciate stare.
1g	3	Lasciate stare.
mcast	2	Impostare su 4 se si utilizza il multicast (CatOS 5.5[5] e versioni successive).
gestione	5	Lasciate stare.
mls	5	Lasciate stare.
pagp	5	Lasciate stare.
profilato	2	Lasciate stare.
potatura	2	Lasciate stare.
Privatevlan	3	Lasciate stare.
qos	3	Lasciate stare.
raggio	2	Lasciate stare.
rsvp	3	Lasciate stare.
sicurezza	2	Lasciate stare.
snmp	2	Lasciate stare.
spanttree	2	Passare a 6.
sys	5	Passare a 6.
tac	2	Lasciate stare.
tcp	2	Lasciate stare.
telnet	2	Lasciate stare.
TFTP	2	Lasciate stare.
UDLD	4	Lasciate stare.
VMPS	2	Lasciate stare.

VTP	2	Lasciate stare.

[1] In CatOS 7.x e versioni successive, il codice dell'impianto etico sostituisce il codice dell'impianto di paging per riflettere il supporto LACP.

Nota: al momento, gli switch Catalyst registrano un messaggio di modifica della configurazione syslog di livello 6 per ciascun comando **set** o **clear** eseguito, a differenza del software Cisco IOS, che attiva il messaggio solo dopo aver chiuso la modalità di configurazione. Se è necessario eseguire il backup delle configurazioni in tempo reale con questo trigger, questi messaggi devono essere inviati anche al server syslog RME. Per la maggior parte dei clienti, sono sufficienti i backup periodici della configurazione per gli switch Catalyst e non è necessario modificare la gravità predefinita della registrazione sul server.

Se si sintonizzano gli avvisi NMS, consultare la Guida ai messaggi di sistema.

Protocollo SCEP (Simple Network Management Protocol)

Il protocollo SNMP viene utilizzato per recuperare le statistiche, i contatori e le tabelle memorizzati nei database MIB (Network Device Management Information Base). Le informazioni raccolte possono essere utilizzate dagli NMS (ad esempio HP Openview) per generare avvisi in tempo reale, misurare la disponibilità e produrre informazioni sulla pianificazione della capacità, nonché per eseguire controlli di configurazione e risoluzione dei problemi.

Panoramica operativa

Con alcuni meccanismi di sicurezza, una stazione di gestione di rete è in grado di recuperare informazioni nei MIB con il protocollo SNMP get e get next request, nonché di modificare i parametri con il comando **set**. È inoltre possibile configurare un dispositivo di rete in modo che generi un messaggio trap per il sistema NMS per l'invio di avvisi in tempo reale. Il polling SNMP utilizza la porta 161 UDP IP e le trap SNMP la porta 162.

Cisco supporta queste versioni di SNMP:

- SNMPv1: RFC 1157 - Standard Internet, uso della protezione delle stringhe della community in testo non crittografato. Un elenco di controllo di accesso con indirizzo IP e una password definiscono la comunità di manager in grado di accedere al MIB dell'agente.
- SNMPv2C: una combinazione di SNMPv2, una bozza di standard Internet definita nelle RFC da 1902 a 1907, e SNMPv2C, una struttura amministrativa basata su community per SNMPv2, una bozza sperimentale definita nella RFC 1901. I vantaggi includono un meccanismo di recupero di massa che supporta il recupero di tabelle e di grandi quantità di informazioni, riduce al minimo il numero di round-trip richiesti e migliora la gestione degli errori.
- SNMPv3: La bozza proposta dalla RFC 2570 fornisce accesso sicuro ai dispositivi tramite la combinazione di autenticazione e crittografia dei pacchetti sulla rete. Le funzioni di sicurezza fornite in SNMPv3 sono:Integrità messaggio: assicura che un pacchetto non sia stato manomesso durante la trasmissioneAutenticazione: determina che il messaggio proviene da un'origine validaCrittografia: codifica il contenuto di un pacchetto per evitare che venga visualizzato facilmente da una fonte non autorizzata

Questa tabella identifica le combinazioni di modelli di sicurezza:

Livello modello	Autenticazione	Crittografia	Risultato
v1	noAuthNoPriv, stringa della community	No	Utilizza una stringa della community per l'autenticazione.
v2c	noAuthNoPriv, stringa della community	No	Utilizza una stringa della community per l'autenticazione.
v3	noAuthNoPriv, nome utente	No	Utilizza un nome utente corrispondente per l'autenticazione.
v3	authNoPriv, MD5 o SHA	Np	Fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA.
v3	authPriv, MD5 o SHA	DES	Fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA. Crittografia DES a 56 bit oltre all'autenticazione basata sullo standard CBC-DES (DES-56).

Nota: tenere presenti queste informazioni sugli oggetti SNMPv3:

- Ogni utente appartiene a un gruppo.
- Un gruppo definisce i criteri di accesso per un gruppo di utenti.
- I criteri di accesso definiscono quali oggetti SNMP sono accessibili per la lettura, la scrittura e la creazione.
- Un gruppo determina l'elenco di notifiche che gli utenti possono ricevere.
- Un gruppo definisce inoltre il modello di protezione e il livello di protezione per i propri utenti.

Consigli sulle trap SNMP

L'SNMP è la base della gestione di tutte le reti ed è abilitato e utilizzato su tutte le reti. L'agente SNMP sullo switch deve essere impostato in modo da utilizzare la versione di SNMP supportata dalla stazione di gestione. Poiché un agente può comunicare con più manager, è possibile configurare il software in modo che supporti la comunicazione con una stazione di gestione che utilizza il protocollo SNMPv1 e un'altra che utilizza il protocollo SNMPv2, ad esempio.

La maggior parte delle stazioni NMS utilizza attualmente SNMPv2C con questa configurazione:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

Cisco consiglia di abilitare le trap SNMP per tutte le funzionalità in uso (le funzionalità non utilizzate possono essere disabilitate, se lo si desidera). Una volta abilitata, la trap può essere verificata con il comando **test snmp** e configurata sul sistema NMS la gestione appropriata per l'errore (ad esempio, un avviso o un popup).

Tutte le trap sono disabilitate per default e devono essere aggiunte alla configurazione, singolarmente o tramite il parametro **all**, come mostrato di seguito:

```
set snmp trap enable all
set snmp trap server address read-only community string
```

Le trap disponibili in CatOS 5.5 includono:

Trap	Descrizione
auth	Autenticazione
ponte	Ponte
telaio	Chassis
config	Configurazione
entità	Entità
ipallow	permesso IP
modulo	Modulo
ripetitore	Ripetitore
stpx	Estensione Spanning Tree
syslog	Notifica Syslog
vmps	Server delle policy di appartenenza della VLAN
vtp	VLAN Trunk Protocol

Nota: la trap del syslog invia tutti i messaggi del syslog generati dallo switch al sistema NMS anche come trap SNMP. Se l'avviso syslog è già stato eseguito da un analizzatore come Cisco Works 2000 RME, non è necessariamente utile ricevere queste informazioni due volte.

A differenza del software Cisco IOS, le trap SNMP a livello di porta sono disabilitate per impostazione predefinita perché gli switch possono avere centinaia di interfacce attive. Cisco consiglia pertanto di abilitare le trap SNMP a livello di porta sulle porte chiave, ad esempio i collegamenti all'infrastruttura a router, switch e server principali. Altre porte, come le porte host degli utenti, non sono necessarie, il che contribuisce a semplificare la gestione della rete.

```
set port trap port range enable
!--- Enable on key ports only.
```

Raccomandazione polling SNMP

Si raccomanda un esame della gestione della rete per discutere in dettaglio le esigenze specifiche. Tuttavia, vengono elencate alcune filosofie di Cisco di base per la gestione di reti di grandi dimensioni:

- Fate qualcosa di semplice, e fatelo bene.
- Ridurre il sovraccarico del personale dovuto a un numero eccessivo di operazioni di polling, raccolta, strumenti e analisi manuali dei dati.
- La gestione della rete è possibile solo con alcuni strumenti, come HP Openview come NMS, Cisco RME come configurazione, syslog, inventario e software manager, Microsoft Excel come analizzatore di dati NMS e CGI come metodo di pubblicazione sul Web.
- La pubblicazione di report sul web consente agli utenti, come ad esempio i senior manager e gli analisti, di accedere alle informazioni senza sovraccaricare il personale operativo con molte richieste speciali.
- Scopri cosa funziona bene sulla rete e lasciala in pace. Concentratevi su ciò che non funziona.

La prima fase dell'implementazione del sistema NMS deve essere quella di basare l'hardware di rete. Si può dedurre molto sullo stato dei dispositivi e dei protocolli dall'utilizzo semplice di CPU, memoria e buffer sui router e dall'utilizzo di CPU, memoria e backplane NMP sugli switch. Solo dopo una linea di base hardware, le linee di base media, picco e carico del traffico L2 e L3 diventano completamente significative. Le baseline vengono in genere stabilite in diversi mesi per ottenere la visibilità dei trend giornalieri, settimanali e trimestrali, in base al ciclo aziendale.

Molte reti soffrono di problemi di prestazioni e capacità NMS causati dall'overpolling. Una volta stabilita la base di riferimento, si consiglia pertanto di impostare le soglie RMON di allarme e di evento sui dispositivi stessi per avvisare il sistema NMS in caso di modifiche anomale e quindi rimuovere il polling. Ciò consente alla rete di comunicare agli operatori quando qualcosa non è normale, piuttosto che continuare a controllare per vedere se tutto è normale. Le soglie possono essere impostate in base a diverse regole, ad esempio il valore massimo più una percentuale o una deviazione standard da una media, e non rientrano nell'ambito del presente documento.

La seconda fase dell'implementazione dell'NMS consiste nel polling di particolari aree della rete in modo più dettagliato con l'SNMP. Ciò include aree di dubbio, aree prima di un cambiamento, o aree che sono caratterizzate come ben funzionanti. Utilizzare i sistemi NMS come luce di ricerca per analizzare la rete in dettaglio e illuminare le aree calde (non tentare di illuminare l'intera rete).

Il gruppo Cisco Network Management Consulting consiglia di analizzare o monitorare i MIB di errori principali nelle reti dei campus. Per ulteriori informazioni, ad esempio sui MIB delle prestazioni da sottoporre a polling, consultare il documento Cisco Network Monitoring and Event Correlation Guidelines.

Nome oggetto	Descrizione oggetto	OID	Intervallo di polling	Soglia
MIB-II				
TempoSuSistema	tempo di attività del sistema in 1/100 di secondo	1.3.6.1.2.1.1.3	5 min.	< 30000

Nome	Descriz	OID	Interv	Soglia

oggetto	ione oggetto		allo di polling	
CISCO-PROCESS-MIB				
cpmCPUTotal5min	Percentuale complessiva di CPU occupata negli ultimi 5 minuti	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 min.	Previsione

Nome oggetto	Descrizione oggetto	OID	Intervallo di polling	Soglia
CISCO-STACK-MIB				
sysAttivaTrapChassis	Indica se devono essere generate trap chassisAlarmOn e chassisAlarmOff in questo MIB.	1.3.6.1.4.1.9.5.1.1.24	24 ore	1
sysEnableModuleTrap	Indica se devono essere generati i trap moduleUp e moduleDown in questo MIB.	1.3.6.1.4.1.9.5.1.1.25	24 ore	1
sysEnableBridgeTrap	Indica se devono essere generate trap newRoot e topologyChange in BRIDGE-MIB (RFC 1493).	1.3.6.1.4.1.9.5.1.1.26	24 ore	1
sysEnableRepeaterTrap	Indica se devono essere generate le trap in REPEATER-MIB (RFC1516).	1.3.6.1.4.1.9.5.1.1.29	24 ore	1
sysEnableIpPermitTrap	Indica se devono essere generate le trap dell'autorizzazione IP in questo MIB.	1.3.6.1.4.1.9.5.1.1.31	24 ore	1
sysAbilitaVmp	Indica se deve	1.3.6.1.4.1.9	24	1

sTrap	essere generata la trap vmVmpsChange definita in CISCO- VLAN-MEMBERSHIP-MIB.	.5.1.1.33	ore	
sysEnableConfigTrap	Indica se deve essere generata la trap sysConfigChange in questo MIB.	1.3.6.1.4.1.9.5.1.1.35	24 ore	1
sysAbilitaIniziTrap	Indica se deve essere generata la trap stpxInconsistencyUpdate in CISCO-STP-EXTENSIONS-MIB.	1.3.6.1.4.1.9.5.1.1.40	24 ore	1
stato chassisPs1	Stato dell'alimentatore 1.	1.3.6.1.4.1.9.5.1.2.4	10 min.	2
chassisPs1RisultatoTest	Informazioni dettagliate sullo stato dell'alimentatore 1.	1.3.6.1.4.1.9.5.1.2.5	Se necessario.	
chassisPs2Status	Stato dell'alimentatore 2.	1.3.6.1.4.1.9.5.1.2.7	10 min.	2
chassisPs2TestResult	Informazioni dettagliate sullo stato dell'alimentatore 2	1.3.6.1.4.1.9.5.1.2.8	Se necessario.	
statoVentolaChassis	Stato della ventola dello chassis.	1.3.6.1.4.1.9.5.1.2.9	10 min.	2
RisultatoTestVentolaChassis	Informazioni dettagliate sullo stato della ventola dello chassis.	1.3.6.1.4.1.9.5.1.2.10	Se necessario.	
chassisMinorAlarm	Stato Dell'Allarme Minore Per Lo Chassis.	1.3.6.1.4.1.9.5.1.2.11	10 min.	1
MajorAlarm dello chassis	Stato allarme principale	1.3.6.1.4.1.9.5.1.2.12	10 min.	1

	chassis			
.TempAlarm dello chassis	Stato di allarme temperatura chassis.	1.3.6.1.4.1.9.5.1.2.13	10 min.	1
StatoModulo	Stato operativo del modulo.	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min.	2
risultatoTestModulo	Informazioni dettagliate sulla condizione dei moduli.	1.3.6.1.4.1.9.5.7.3.1.1.11	Se necessario.	
.StatoStandbyModulo	Stato di un modulo ridondante.	1.3.6.1.4.1.9.5.7.3.1.1.21	30 min.	=1 o =4

Nome oggetto	Descrizione oggetto	OID	Intervallo di polling	Soglia
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	Tempo (in 1/100 sec) trascorso dall'ultima volta in cui l'entità ha rilevato una modifica della topologia.	1.3.6.1.2.1.17.2.3	5 min.	< 30000
dot1dStpTopChanges	Numero totale di modifiche alla topologia rilevate dal bridge dall'ultima reimpostazione o inizializzazione dell'entità di gestione.	1.3.6.1.2.1.17.2.4	Se necessario.	
dot1dStpPortState [1]	Lo stato corrente della porta come definito dall'applicazione dello Spanning	1.3.6.1.2.1.17.2.15.1.3	Se necessario.	

	Tree Protocol. Il valore restituito può essere uno dei seguenti: `disabilitato (1), bloccante (2), in ascolto (3), in apprendimento (4), in inoltro (5)` o `interrotto (6)`.			

Nome oggetto	Descrizione oggetto	OID	Intervallo di polling	Soglia
CISCO-MEMORY-POOL-MIB				
UtilizzoPoolMemoriaCisco	Indica il numero di byte del pool di memoria attualmente utilizzati dalle applicazioni sul dispositivo gestito.	1.3.6.1.4.1.9.9.48.1.1.1.5	30 min.	Previsione
ciscoMemoryPoolFree	Indica il numero di byte del pool di memoria attualmente inutilizzati nel dispositivo gestito. **Nota:** la somma di ciscoMemoryPoolUsed e ciscoMemoryPoolFree è la quantità totale di memoria nel pool.	1.3.6.1.4.1.9.9.48.1.1.1.6	30 min.	Previsione
CiscoMemoryPoolLargestFree	Indica il numero massimo di byte contigui	1.3.6.1.4.1.9.9.48.1.1.1.7	30 min.	Previsione

	dal pool di memoria attualmente inutilizzati nel dispositivo gestito.			

Per ulteriori informazioni sul supporto dei MIB Cisco, fare riferimento a Cisco Network Management Toolkit - MIB.

Nota: alcuni MIB standard presuppongono che una particolare entità SNMP contenga solo un'istanza del MIB. Pertanto, il MIB standard non dispone di alcun indice che consenta agli utenti di accedere direttamente a una particolare istanza del MIB. In questi casi, viene fornita l'indicizzazione della stringa della community per accedere a ciascuna istanza del MIB standard. La sintassi è [stringa della community]@[numero istanza], dove istanza è in genere un numero VLAN.

Altre opzioni

Gli aspetti relativi alla sicurezza di SNMPv3 indicano che il suo utilizzo dovrebbe superare SNMPv2 nel tempo. Cisco consiglia ai clienti di prepararsi per questo nuovo protocollo come parte della strategia NMS. I vantaggi sono che i dati possono essere raccolti in modo sicuro dai dispositivi SNMP senza il rischio di manomissione o danneggiamento. Le informazioni riservate, ad esempio i pacchetti del comando **set** SNMP che modificano la configurazione di uno switch, possono essere crittografate per impedire che il loro contenuto venga esposto sulla rete. Inoltre, gruppi di utenti diversi possono disporre di privilegi diversi.

Nota: la configurazione di SNMPv3 è significativamente diversa dalla riga di comando di SNMPv2 e si prevede un aumento del carico della CPU sul Supervisor Engine.

Monitoraggio remoto

RMON consente ai dati MIB di essere pre-elaborati dal dispositivo di rete stesso, in preparazione ad usi comuni o all'applicazione di tali informazioni da parte del gestore della rete, come l'esecuzione di una determinazione cronologica della linea di base e di un'analisi delle soglie.

I risultati dell'elaborazione RMON vengono memorizzati nei MIB RMON per la successiva raccolta da parte di un NMS, come definito nella RFC 1757 .

Panoramica operativa

Gli switch Catalyst supportano i comandi mini-RMON nell'hardware di ciascuna porta, costituita da quattro gruppi RMON-1 di base: Statistiche (gruppo 1), Cronologia (gruppo 2), Allarmi (gruppo 3) ed Eventi (gruppo 9).

La parte più potente di RMON-1 è il **meccanismo di soglia** fornito dai gruppi di **allarme e di eventi**. Come accennato in precedenza, la configurazione delle soglie RMON consente allo switch di inviare una trap SNMP quando si verifica una condizione anomala. Dopo aver identificato le porte chiave, è possibile usare il protocollo SNMP per eseguire il polling dei contatori o dei gruppi di cronologia RMON e creare linee di base per registrare le normali attività di traffico per tali porte. Successivamente, è possibile impostare le soglie di innalzamento e abbassamento dei valori

RMON e configurare gli allarmi in caso di variazione definita rispetto alla baseline.

La configurazione delle soglie può essere eseguita in modo ottimale con un pacchetto di gestione RMON, in quanto la corretta creazione delle righe di parametri nelle tabelle degli allarmi e degli eventi è un'operazione noiosa. I pacchetti RMON NMS commerciali, ad esempio Cisco Traffic Director e parte di Cisco Works 2000, includono interfacce utente che semplificano notevolmente l'impostazione delle soglie RMON.

Per scopi di base, il gruppo therStats fornisce un utile intervallo di statistiche del traffico L2. Gli oggetti di questa tabella possono essere utilizzati per ottenere statistiche sul traffico unicast, multicast e broadcast, nonché una serie di errori L2. L'agente RMON sullo switch può essere configurato anche per memorizzare i valori campionati nel gruppo di cronologia. Questo meccanismo consente di ridurre la quantità di polling senza ridurre la frequenza di campionamento. Le cronologie RMON possono fornire linee di base accurate senza un sostanziale sovraccarico del polling. Tuttavia, più cronologie vengono raccolte, maggiore è il numero di risorse utilizzate per lo switch.

Mentre gli switch forniscono solo quattro gruppi base di RMON-1, è importante non dimenticare il resto di RMON-1 e RMON-2. Tutti i gruppi sono definiti nella RFC 2021, tra cui UserHistory (gruppo 18) e ProbeConfig (gruppo 19). È possibile recuperare informazioni di livello 3 e superiori dagli switch con la porta SPAN o le funzionalità di reindirizzamento degli ACL della VLAN, in modo da copiare il traffico su uno switch Probe RMON esterno o su un Network Analysis Module (NAM) interno.

I nomi supportano tutti i gruppi RMON e possono esaminare anche **i dati a livello di applicazione**, inclusi i dati Netflow esportati dai Catalyst quando MLS è abilitato. Se si esegue MLS, il router non commuta tutti i pacchetti del flusso, quindi solo l'esportazione dei dati Netflow e non i contatori dell'interfaccia danno un accounting VLAN affidabile.

Èpossibile usare una porta SPAN e una sonda dello switch per acquisire un flusso di pacchetti per una particolare porta, trunk o VLAN e caricare i pacchetti per decodificarli con un pacchetto di gestione RMON. La porta SPAN è controllabile da SNMP tramite il gruppo SPAN in CISCO-STACK-MIB, quindi questo processo è facile da automatizzare. Traffic Director utilizza queste funzionalità con la funzionalità di agente di trasporto.

Esistono alcune avvertenze sull'estensione di un'intera VLAN. Anche se si utilizza una sonda da 1 Gbps, l'intero flusso di pacchetto da una VLAN o anche da una porta full-duplex da 1 Gbps può superare la larghezza di banda della porta SPAN. Se la porta SPAN è in esecuzione a larghezza di banda piena, è possibile che i dati vengano persi. Per ulteriori informazioni, fare riferimento a Configurazione della funzionalità Catalyst Switched Port Analyzer (SPAN).

Suggerimento

Cisco consiglia di implementare le soglie RMON e gli avvisi per una gestione della rete più intelligente del solo polling SNMP. Ciò riduce il sovraccarico del traffico di gestione della rete e consente alla rete di inviare un avviso intelligente quando qualcosa è cambiato rispetto alla linea di base. il sistema RMON deve essere gestito da un agente esterno, quale il Traffic Director; non è disponibile il supporto CLI. Per abilitare RMON, eseguire questi comandi:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
```

```
!--- For use with NAM module only.
```

Èimportante ricordare che la funzione principale di uno switch è inoltrare i frame, non agire come una sonda RMON su più porte di grandi dimensioni. Pertanto, quando si impostano cronologie e soglie su più porte per più condizioni, tenere presente che le risorse vengono utilizzate. Se si sta eseguendo il ridimensionamento di RMON, è consigliabile utilizzare un modulo NAM. Tenere inoltre presente la regola della porta critica: eseguire il polling e impostare le soglie solo sulle porte identificate come importanti nella fase di pianificazione.

Requisiti di memoria

L'utilizzo della memoria RMON è costante su tutte le piattaforme di switch in relazione a statistiche, storie, allarmi ed eventi. RMON utilizza un bucket per archiviare le cronologie e le statistiche sull'agente RMON (in questo caso lo switch). Le dimensioni del bucket vengono definite sulla sonda RMON (sonda dello switch) o sull'applicazione RMON (Traffic Director), quindi inviate allo switch per essere impostate. In genere, i vincoli di memoria sono considerati solo sui Supervisor Engine meno recenti con meno di 32 MB di DRAM. Fare riferimento alle seguenti linee guida:

- All'immagine NMP vengono aggiunti circa 450 K di spazio di codice per il supporto dei mini-RMON (ovvero quattro gruppi di RMON: statistiche, cronologia, allarmi ed eventi). I requisiti di memoria dinamica per RMON variano perché dipendono dalla configurazione in fase di esecuzione. Le informazioni sull'utilizzo della memoria RMON in fase di esecuzione per ciascun gruppo mini-RMON sono descritte di seguito:Ethernet Statistics group: richiede 800 byte per ciascuna interfaccia Ethernet/FE commutata.Gruppo cronologia: per l'interfaccia Ethernet, ogni voce di controllo della cronologia configurata con 50 bucket richiede circa 3,6 KB di spazio di memoria e 56 byte per ogni bucket aggiuntivo.Gruppi di allarmi ed eventi: sono necessari 2,6 KB per ogni allarme configurato e per le voci di evento corrispondenti.
- Per salvare la configurazione relativa a RMON, sono necessari circa 20 K di NVRAM se le dimensioni totali della NVRAM del sistema sono pari a 256 K o più e 10 K di spazio NVRAM se le dimensioni totali della NVRAM sono pari a 128 K.

Protocollo orario di rete

L'NTP, RFC 1305 , sincronizza la temporizzazione tra una serie di client e time server distribuiti e consente di correlare gli eventi quando vengono creati i registri di sistema o si verificano altri eventi specifici dell'ora.

L'NTP fornisce precisione negli orari dei client, generalmente entro un millisecondo sulle LAN e fino a qualche decina di millisecondi sulle WAN, relativamente a un server primario sincronizzato con l'ora UTC (Coordinated Universal Time). Le configurazioni NTP tipiche utilizzano più server ridondanti e percorsi di rete diversi per ottenere un alto livello di accuratezza e affidabilità. Alcune configurazioni includono l'autenticazione crittografica per impedire attacchi accidentali o dannosi al protocollo.

Panoramica operativa

Il protocollo NTP è stato documentato per la prima volta nella RFC 958 , ma si è evoluto attraverso la RFC 1119 (NTP versione 2) ed è ora nella terza versione come definito nella RFC 1305 . Funziona sulla porta UDP 123. Tutte le comunicazioni NTP utilizzano l'ora UTC, che corrisponde all'ora di Greenwich.

Accesso ai server di riferimento orario pubblici

La subnet NTP attualmente include oltre 50 server primari pubblici sincronizzati direttamente con UTC via radio, satellite o modem. In genere, le workstation client e i server con un numero relativamente ridotto di client non vengono sincronizzati con i server principali. Esistono circa 100 server secondari pubblici sincronizzati con i server primari che forniscono la sincronizzazione a oltre 100.000 client e server su Internet. Gli elenchi correnti vengono gestiti nella pagina Elenco dei server NTP pubblici, che viene aggiornata regolarmente. Esistono numerosi server primari e secondari privati che normalmente non sono disponibili anche per il pubblico. Per un elenco dei server NTP pubblici e informazioni su come utilizzarli, consultare il sito Web della University of Delaware Time Synchronization Server .

Poiché non vi è alcuna garanzia che questi server NTP Internet pubblici saranno disponibili o che producono l'ora corretta, si consiglia vivamente di prendere in considerazione altre opzioni. Ciò potrebbe includere l'uso di vari dispositivi GPS (Global Positioning Service) indipendenti collegati direttamente a un certo numero di router.

Un'altra opzione possibile è l'uso di vari router configurati come master di Stratum 1, anche se questa operazione non è consigliata.

Strato

Ogni server NTP adotta uno strato che indica quanto lontano si trova il server da una fonte di tempo esterna. I server di Stratum 1 hanno accesso a una fonte di tempo esterna, ad esempio un orologio radio. I server di Stratum 2 ottengono i dettagli temporali da un insieme designato di server di Stratum 1, mentre i server di Stratum 3 ottengono i dettagli temporali dai server di Stratum 2 e così via.

Relazione peer server

- Per server si intende un server che risponde alle richieste dei client, ma che non tenta di incorporare informazioni sulla data provenienti da un'origine ora client.
- Un peer risponde alle richieste del client, ma tenta di utilizzare le richieste del client come potenziale candidato per una fonte di tempo migliore e per aiutare a stabilizzare la sua frequenza di clock.
- Per essere un vero peer, entrambi i lati della connessione devono entrare in una relazione peer anziché avere un utente come peer e l'altro utente come server. È inoltre consigliabile che i peer scambino le chiavi in modo che solo gli host attendibili possano comunicare tra loro come peer.
- In una richiesta client a un server, il server risponde al client e dimentica che il client ha mai posto una domanda; in una richiesta del client a un peer, il server risponde al client e conserva le informazioni sullo stato relative al client per tenere traccia delle prestazioni del client durante la gestione dei tempi e dello strato server in esecuzione.**Nota:** CatOS può funzionare solo come client NTP.

Per un server NTP non è un problema gestire migliaia di client. Tuttavia, la gestione di centinaia di peer ha un impatto sulla memoria e la manutenzione dello stato comporta un consumo maggiore di risorse della CPU sulla scatola e sulla larghezza di banda.

Sondaggio

Il protocollo NTP consente a un client di eseguire query su un server in qualsiasi momento. Infatti, quando il protocollo NTP viene configurato per la prima volta in un dispositivo Cisco, invia otto query in rapida successione a intervalli NTP_MINPOLL (24 = 16 secondi). NTP_MAXPOLL è di 214 secondi (ossia 16.384 secondi o 4 ore, 33 minuti, 4 secondi), il tempo massimo necessario prima che NTP esegua nuovamente il polling per ottenere una risposta. Al momento, Cisco non dispone di un metodo per forzare manualmente l'impostazione dell'ora POLL da parte dell'utente.

Il contatore di polling NTP inizia a 2^6 (64) secondi e viene incrementato dalla potenza di due (quando i due server si sincronizzano tra loro) a 2^{10}. Ciò significa che i messaggi di sincronizzazione devono essere inviati a un intervallo di 64, 128, 256, 512 o 1024 secondi per server o peer configurato. Il tempo varia tra 64 secondi e 1024 secondi alla potenza di due, in base al loop con blocco di fase che invia e riceve i pacchetti. Se c'è molto tremore nel tempo, sondaggi più spesso. Se l'orologio di riferimento è accurato e la connettività di rete è coerente, i tempi di polling convergono in 1024 secondi tra ogni polling.

Nel mondo reale, questo significa che l'intervallo di polling NTP cambia quando cambia la connessione tra il client e il server. Migliore è la connessione, maggiore è l'intervallo di polling, il che significa che il client NTP ha ricevuto otto risposte per le ultime otto richieste (l'intervallo di polling viene quindi raddoppiato). In caso di mancata risposta singola, l'intervallo di polling viene dimezzato. L'intervallo di polling inizia a 64 secondi e arriva a un massimo di 1024 secondi. Nelle circostanze più favorevoli, l'intervallo di polling impiega poco più di due ore per passare da 64 secondi a 1024 secondi.

Trasmissioni

Le trasmissioni NTP non vengono mai inoltrate. Il comando **ntp broadcast** determina l'origine dei broadcast NTP del router sull'interfaccia su cui è configurato. Il comando **ntp broadcast client** determina che il router o lo switch ascolti i broadcast NTP sull'interfaccia su cui è configurato.

Livelli di traffico NTP

La larghezza di banda utilizzata dall'NTP è minima, in quanto l'intervallo tra i messaggi di polling scambiati tra peer in genere ritorna a non più di un messaggio ogni 17 minuti (1024 secondi). Con un'attenta pianificazione, questa condizione può essere mantenuta all'interno delle reti di router sui collegamenti WAN. I client NTP devono eseguire il peer verso i server NTP locali, non attraverso la WAN fino ai router centrali del sito che saranno i server di strato 2.

Un client NTP convergente utilizza circa 0,6 bit/secondo per server.

Suggerimento

Molti clienti hanno NTP configurato oggi in modalità client sulle loro piattaforme CatOS, sincronizzato da diversi feed affidabili da Internet o da un orologio radio. Tuttavia, un'alternativa più semplice alla modalità server quando si utilizza un numero elevato di switch è abilitare il protocollo NTP in modalità client di trasmissione sulla VLAN di gestione di un dominio commutato. Questo meccanismo consente a un intero dominio di Catalyst di ricevere un orologio da un singolo messaggio broadcast. Tuttavia, l'accuratezza della gestione dei tempi è ridotta marginalmente perché il flusso di informazioni è unidirezionale.

Anche l'utilizzo degli indirizzi di loopback come origine degli aggiornamenti può contribuire alla coerenza. I problemi di sicurezza possono essere affrontati in due modi:

- Filtraggio degli aggiornamenti del server
- Autenticazione

La correlazione temporale degli eventi è estremamente utile in due casi: risoluzione dei problemi e controlli di sicurezza. È necessario prestare attenzione per proteggere le origini del tempo e i dati. Si consiglia di utilizzare la crittografia in modo che gli eventi chiave non vengano cancellati intenzionalmente o involontariamente.

Cisco consiglia le seguenti configurazioni:

Configurazione Catalyst

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone
```

Configurazione Catalyst Alternativa

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Configurazione router

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

Protocollo Cisco Discovery

Il CDP scambia informazioni tra dispositivi adiacenti sul layer di collegamento dati ed è estremamente utile per determinare la topologia di rete e la configurazione fisica all'esterno del layer logico o IP. I dispositivi supportati sono principalmente switch, router e telefoni IP. In questa sezione vengono evidenziati alcuni dei miglioramenti apportati alla versione 2 di CDP rispetto alla versione 1.

Panoramica operativa

Il CDP utilizza l'incapsulamento SNAP con codice di tipo 2000. Su Ethernet, ATM e FDDI, viene utilizzato l'indirizzo multicast di destinazione **01-00-0c-cc-cc-cc, tipo di protocollo HDLC 0x2000**. Sui Token Ring, viene utilizzato l'indirizzo funzionale c000.0800.0000. Per impostazione predefinita, i frame CDP vengono inviati periodicamente ogni minuto.

I messaggi CDP contengono uno o più messaggi secondari che consentono ai dispositivi di destinazione di raccogliere e archiviare informazioni su tutti i dispositivi adiacenti.

CDP versione 1 supporta i seguenti parametri:

Parametro	Tipo	Descrizione
1	ID dispositivo	Nome host del dispositivo o numero di serie dell'hardware in ASCII.
2	Indirizzo	Indirizzo L3 dell'interfaccia che ha inviato l'aggiornamento.
3	Port-ID	Porta a cui è stato inviato l'aggiornamento CDP.
4	Funzionalità	Descrive le funzionalità del dispositivo: Router: Bridge 0x01 TB: 0x02 Adattatore SR: Switch 0x04: 0x08 (fornisce switching L2 e/o L3) Host: Filtraggio condizionale 0x10 IGMP: 0x20 Il bridge o lo switch non inoltrano i pacchetti di report IGMP su porte non router. Ripetitore: 0x40
5	Version	Stringa di caratteri contenente la versione del software (come in **show version**).
6	Piattaforma	Piattaforma hardware, ad esempio WS-C5000, WS-C6009 o Cisco RSP.

Nella versione 2 del CDP sono stati introdotti campi di protocollo aggiuntivi. CDP versione 2 supporta qualsiasi campo, ma quelli elencati possono essere particolarmente utili in ambienti a commutazione e sono utilizzati in CatOS.

Nota: Quando uno switch esegue CDPv1, elimina i frame v2. Quando uno switch con CDPv2 riceve un frame CDPv1 su un'interfaccia, inizia a inviare frame CDPv1 fuori da quell'interfaccia, oltre a frame CDPv2.

Parametro	Tipo	Descrizione
9	Dominio VTP	Il dominio VTP, se configurato sul dispositivo.
10	VLAN nativa	Nel dot1q, questa è la VLAN senza tag.
11	Full/Half Duplex	Questo campo contiene l'impostazione duplex della porta di invio.

Suggerimento

Il CDP è abilitato per impostazione predefinita ed è essenziale per ottenere la visibilità dei dispositivi adiacenti e per la risoluzione dei problemi. Viene inoltre utilizzato dalle applicazioni di gestione della rete per creare mappe della topologia L2. Per configurare il CDP, eseguire questi comandi:

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

Nelle parti della rete in cui è richiesto un elevato livello di sicurezza (ad esempio le DMZ con connessione Internet), il CDP deve essere spento come tale:

```
set cdp disable port range
```

Il comando show cdp neighbors visualizza la tabella CDP locale. Le voci contrassegnate con un asterisco (*) indicano una mancata corrispondenza della VLAN; le voci contrassegnate da # indicano una mancata corrispondenza del duplex. Ciò può essere utile per la risoluzione dei problemi.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ----------------- ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Altre opzioni

Alcuni switch, come Catalyst 6500/6000, sono in grado di fornire alimentazione ai telefoni IP tramite cavi UTP. Le informazioni ricevute tramite il CDP contribuiscono al risparmio energia sullo switch.

Poiché ai telefoni IP può essere collegato un PC ed entrambi i dispositivi si connettono alla stessa porta sul Catalyst, lo switch ha la possibilità di collegare il telefono VoIP a una VLAN separata, l'accessorio. Ciò consente allo switch di applicare facilmente una diversa QoS (Quality of Service) per il traffico VoIP.

Inoltre, se si modifica la VLAN ausiliaria (ad esempio, per forzare il telefono a usare una VLAN specifica o un metodo di tag specifico), queste informazioni vengono inviate al telefono con il CDP.

Parametro	Tipo	Descrizione
14	ID accessorio	Consente di distinguere il traffico VoIP da altro traffico, ad esempio da una VLAN-id (VLAN ausiliaria) separata.

16	Consumo	Quantità di energia utilizzata da un telefono VoIP, in milliwatt.

Nota: gli switch Catalyst 2900 e 3500XL non supportano CDPv2.

Configurazione protezione

Idealmente, il cliente ha già stabilito una policy di sicurezza per aiutare a definire quali strumenti e tecnologie Cisco sono qualificati.

Nota: la sicurezza del software Cisco IOS, a differenza di CatOS, è trattata in molti documenti, ad esempio Cisco ISP Essentials.

Funzioni di sicurezza di base

Password

Configurare una password a livello utente (accesso). Le password fanno distinzione tra maiuscole e minuscole in CatOS 5.x e versioni successive e possono avere una lunghezza compresa tra 0 e 30 caratteri, inclusi gli spazi. Impostare la password di abilitazione:

```
set password password set enablepass password
```

Tutte le password devono soddisfare gli standard di lunghezza minima (ad esempio almeno sei caratteri, una combinazione di lettere e numeri, lettere maiuscole e minuscole) per l'accesso e abilitare le password quando utilizzate. Queste password vengono crittografate utilizzando l'algoritmo hash MD5.

Per consentire una maggiore flessibilità nella gestione della sicurezza della password e dell'accesso ai dispositivi, Cisco consiglia di utilizzare un server TACACS+. Per ulteriori informazioni, fare riferimento alla sezione TACACS+ di questo documento.

Secure Shell

Utilizzare la crittografia SSH per garantire la sicurezza delle sessioni Telnet e di altre connessioni remote allo switch. La crittografia SSH è supportata solo per gli accessi remoti allo switch. Non è possibile crittografare sessioni Telnet avviate dallo switch. SSH v1 è supportato in CatOS 6.1, la versione 2 in CatOS 8.3. SSH v1 supporta i metodi di crittografia Data Encryption Standard (DES) e Triple-DES (3-DES), mentre SSH v2 supporta i metodi di crittografia 3-DES e Advanced Encryption Standard (AES). La crittografia SSH può essere utilizzata con l'autenticazione RADIUS e TACACS+. Questa funzione è supportata con le immagini SSH (k9). Per ulteriori informazioni, consultare il documento sulla configurazione del protocollo SSH sugli switch Catalyst con CatOS.

```
set crypto key rsa 1024
```

Per disabilitare il fallback della versione 1 e accettare le connessioni della versione 2, eseguire

questo comando:

```
set ssh mode v2
```

Filtri autorizzazioni IP

Si tratta di filtri per salvaguardare l'accesso all'interfaccia sc0 di gestione tramite Telnet e altri protocolli. Queste impostazioni sono particolarmente importanti quando la VLAN usata per la gestione contiene anche utenti. Per abilitare il filtro indirizzi IP e porte, eseguire questi comandi:

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

Tuttavia, se l'accesso Telnet è limitato con questo comando, l'accesso ai dispositivi CatOS può essere ottenuto solo tramite poche stazioni terminali attendibili. Questa impostazione può rappresentare un ostacolo nella risoluzione dei problemi. Tenere presente che è possibile contraffare gli indirizzi IP e ingannare l'accesso filtrato, quindi questo è solo il primo livello di protezione.

Sicurezza porta

Prendere in considerazione l'uso della funzione di sicurezza delle porte per consentire solo uno o più indirizzi MAC noti per il trasferimento dei dati su una determinata porta (ad esempio, per impedire che le stazioni terminali statiche vengano sostituite con nuove stazioni senza controllo delle modifiche). Questa operazione è possibile mediante indirizzi MAC statici.

```
set port security mod/port enable MAC address
```

Questo è possibile anche imparando dinamicamente gli indirizzi MAC con restrizioni.

```
set port security port range enable
```

Èpossibile configurare le seguenti opzioni:

- set port security *mod/port* age *time value*: specifica per quanto tempo gli indirizzi sulla porta vengono protetti prima che sia possibile apprendere un nuovo indirizzo. L'intervallo valido in minuti è compreso tra 10 e 1440. L'impostazione predefinita è nessuna misurazione durata.
- set port *securitymod/valore* massimo *porta: parola chiave che specifica il numero massimo di indirizzi MAC da proteggere sulla porta.* I valori validi sono 1 (valore predefinito) - 1025.
- set port security *mod/*violazione *porta* shutdown: chiude la porta (impostazione predefinita) se si verifica una violazione, invia un messaggio syslog (impostazione predefinita) e scarta il traffico.
- set port security *mod/port* shutdown *time value (valore di tempo di arresto della porta*

impostato): durata della disabilitazione di una porta. I valori validi sono compresi tra 10 e 1440 minuti. Il valore predefinito è shutdown permanente

Con CatOS 6.x e versioni successive, Cisco ha introdotto l'autenticazione 802.1x che consente ai client di autenticarsi su un server centrale prima che le porte possano essere abilitate per i dati. Questa funzionalità è nelle prime fasi del supporto su piattaforme quali Windows XP, ma può essere considerata una direzione strategica da molte aziende. Per informazioni su come configurare la sicurezza delle porte sugli switch con software Cisco IOS, fare riferimento a Configurazione della sicurezza delle porte.

Banner di accesso

Creare banner appropriati per i dispositivi per indicare in modo specifico le azioni intraprese per l'accesso non autorizzato. Non annunciare il nome del sito o i dati di rete che potrebbero fornire informazioni a utenti non autorizzati. Questi banner offrono il ricorso in caso di danneggiamento di un dispositivo e di cattura dell'aggressore:.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Sicurezza fisica

I dispositivi non devono essere accessibili fisicamente senza un'autorizzazione adeguata, quindi le apparecchiature devono trovarsi in uno spazio controllato (bloccato). per garantire che la rete rimanga operativa e non sia danneggiata da manomissioni dannose di fattori ambientali, tutte le apparecchiature devono disporre di un gruppo di continuità (se possibile con sorgenti ridondanti) e di un controllo della temperatura (condizionamento dell'aria) adeguati. Tenere presente che se l'accesso fisico viene violato da una persona con intenzioni dannose, è molto più probabile che si verifichino interruzioni tramite il recupero della password o altri metodi.

Sistema di controllo di accesso di Terminal Access Controller

Per impostazione predefinita, le password senza privilegi e in modalità privilegiata sono globali e si applicano a tutti gli utenti che accedono allo switch o al router, dalla porta della console o tramite una sessione Telnet in rete. La loro implementazione sui dispositivi di rete è un'operazione lunga e non centralizzata. Inoltre, è difficile implementare le restrizioni di accesso utilizzando elenchi che possono essere soggetti a errori di configurazione.

Sono disponibili tre sistemi di sicurezza per il controllo e la sorveglianza dell'accesso ai dispositivi di rete. Questi sistemi utilizzano architetture client/server per collocare tutte le informazioni sulla sicurezza in un unico database centrale. Questi tre sistemi di sicurezza sono:

- TACACS+
- RAGGIO
- Kerberos

TACACS+ è un'implementazione comune nelle reti Cisco ed è l'argomento principale di questo capitolo. Offre le seguenti funzioni:

- Autenticazione: processo di identificazione e verifica per un utente. È possibile utilizzare diversi metodi per autenticare un utente, ma il più comune include una combinazione di nome utente e password.
- Autorizzazione: è possibile concedere vari comandi dopo l'autenticazione di un utente.
- Accounting: la registrazione di ciò che un utente sta facendo o ha fatto sul dispositivo.

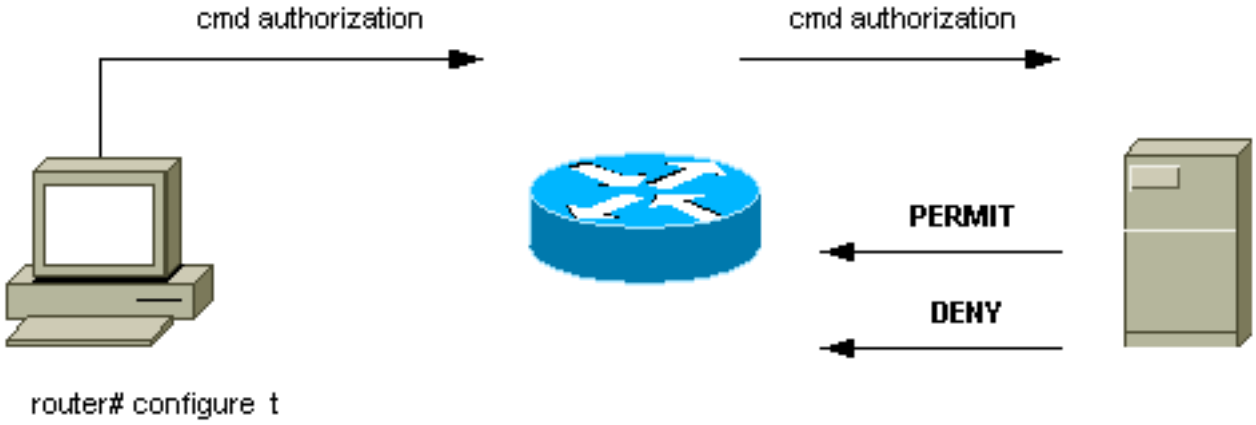
Per ulteriori informazioni, fare riferimento a Configurazione di TACACS+, RADIUS e Kerberos sugli switch Cisco Catalyst.

Panoramica operativa

Il protocollo TACACS+ inoltra nomi utente e password al server centralizzato, crittografato sulla rete tramite hashing unidirezionale **MD5** (RFC 1321). Utilizza la porta TCP 49 come protocollo di trasporto; rispetto a UDP (utilizzato da RADIUS), questa caratteristica offre i seguenti vantaggi:

- Trasporto orientato alle connessioni
- Conferma separata della ricezione di una richiesta (TCP ACK), indipendentemente dal modo in cui è stato caricato il meccanismo di autenticazione back-end
- Indicazione immediata di un arresto anomalo del server (pacchetti RST)

Se durante una sessione è necessario un ulteriore controllo delle autorizzazioni, lo switch controlla con TACACS+ se all'utente è stata concessa l'autorizzazione a utilizzare un particolare comando. In questo modo è possibile controllare meglio i comandi che possono essere eseguiti sullo switch mentre si disconnette dal meccanismo di autenticazione. Utilizzando l'accounting dei comandi, è possibile controllare i comandi emessi da un utente specifico mentre è collegato a un determinato dispositivo di rete.



Quando un utente tenta di eseguire un accesso ASCII semplice autenticandosi a un dispositivo di rete con TACACS+, questo processo si verifica in genere:

- Una volta stabilita la connessione, lo switch contatta il daemon TACACS+ per ottenere un prompt con il nome utente, che viene quindi visualizzato all'utente. L'utente immette un nome utente e lo switch contatta il daemon TACACS+ per ottenere una richiesta della password. Lo switch visualizza la richiesta della password all'utente, che immette una password che viene inviata anche al daemon TACACS+.
- Il dispositivo di rete riceve infine una delle seguenti risposte dal daemon TACACS+:ACCEPT - l'utente viene autenticato e il servizio può iniziare. Se il dispositivo di rete è configurato per richiedere l'autorizzazione, l'autorizzazione inizia in questo momento.REJECT: l'utente non ha eseguito l'autenticazione. All'utente può essere negato un ulteriore accesso o gli viene richiesto di riprovare la sequenza di accesso a seconda del daemon TACACS+.ERRORE: si è

verificato un errore durante l'autenticazione. A tal fine, è possibile utilizzare il daemon o la connessione di rete tra il daemon e lo switch. Se viene ricevuta una risposta di errore, il dispositivo di rete tenta in genere di utilizzare un metodo alternativo per autenticare l'utente.CONTINUE - All'utente vengono richieste informazioni di autenticazione aggiuntive.

- Prima di procedere all'autorizzazione TACACS+, gli utenti devono completare correttamente l'autenticazione TACACS+.
- Se è necessaria l'autorizzazione TACACS+, il daemon TACACS+ viene nuovamente contattato e restituisce una risposta di autorizzazione ACCEPT o REJECT. Se viene restituita una risposta ACCEPT, la risposta contiene dati sotto forma di attributi utilizzati per indirizzare la sessione EXEC o NETWORK per l'utente e per determinare i comandi a cui l'utente può accedere.

Suggerimento

Cisco consiglia di utilizzare TACACS+, in quanto può essere implementato facilmente con Cisco Secure ACS per NT, Unix o altri software di terze parti. Le funzionalità di TACACS+ includono funzionalità di accounting dettagliato per fornire statistiche sull'utilizzo dei comandi e del sistema, algoritmo di crittografia MD5 e controllo amministrativo dei processi di autenticazione e autorizzazione.

Nell'esempio, le modalità di accesso e abilitazione usano il server TACACS+ per l'autenticazione e possono eseguire il fallback all'autenticazione locale se il server non è disponibile. Si tratta di una porta secondaria importante da lasciare nella maggior parte delle reti. Utilizzare questi comandi per configurare TACACS+:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Altre opzioni

Èpossibile usare l'autorizzazione TACACS+ per controllare i comandi che ciascun utente o gruppo di utenti può eseguire sullo switch, ma è difficile consigliare uno switch perché tutti i clienti hanno requisiti specifici in quest'area. per ulteriori informazioni, fare riferimento a Controllo dell'accesso allo switch tramite autenticazione, autorizzazione e accounting.

Infine, i comandi di accounting forniscono un audit trail di ciò che ogni utente ha digitato e configurato. Questo è un esempio che utilizza la pratica comune di ricevere le informazioni di controllo alla fine del comando:

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
```

```
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Questa configurazione dispone delle seguenti funzionalità:

- Il comando **connect** attiva l'accounting degli eventi di connessione in uscita sullo switch, ad esempio Telnet.
- Il comando **exec** abilita l'accounting delle sessioni di accesso sullo switch, ad esempio il personale operativo.
- Il comando **system** permette di registrare gli eventi di sistema sullo switch, ad esempio il riavvio o il reset.
- Il comando **commands** consente di eseguire l'accounting di ciò che è stato immesso sullo switch, sia per il comando **show** che per il comando di configurazione.
- *Aggiornamenti* periodici al server ogni minuto sono utili per registrare se gli utenti sono ancora connessi.

Elenco di controllo della configurazione

In questa sezione viene fornito un riepilogo delle configurazioni consigliate, esclusi i dettagli sulla sicurezza.

Èestremamente utile etichettare tutte le porte. Per assegnare un'etichetta alle porte, usare questo comando:

```
set port description descriptive name
```

Utilizzare questa chiave insieme alle tabelle dei comandi elencate:

Chiave:
Testo in grassetto - modifica consigliata
Testo normale - predefinito, impostazione consigliata

Comandi di configurazione globali

Comando	**Commento**
set vtp domain *name passwordx*	Protezione contro gli aggiornamenti VTP non autorizzati da nuovi switch.
impostazione vtp mode transparent	Selezionare la modalità VTP innalzata di livello in questo documento. Per ulteriori informazioni, consultare la sezione Protocollo VLAN Trunking di questo documento.
imposta spantree attiva tutto	Verificare che STP sia abilitato su tutte le VLAN.
set spanttree root *vlan*	Si consiglia di posizionare i

	bridge radice (e radice secondaria) per VLAN.
impostare spantree backbonefast enable	Abilitare la convergenza STP rapida da errori indiretti (solo se tutti gli switch nel dominio supportano questa funzione).
impostare spantree uplinkfast enable	Convergenza STP rapida da guasti diretti (solo per switch del livello di accesso).
impostare spantree portfast bpdu-guard enable	Abilita la chiusura automatica della porta in caso di estensione Spanning Tree non autorizzata.
set udld enable	Abilitare il rilevamento dei collegamenti unidirezionali (è necessaria anche la configurazione a livello di porta).
impostazione diaglevel test completata	Abilitare la diagnostica completa all'avvio (impostazione predefinita su Catalyst 4500/4000).
set test packetbuffer sun 3:30	Abilitare il controllo degli errori del buffer della porta (solo per Catalyst 5500/5000).
set logging buffer 500	Mantenere il massimo buffer syslog interno.
impostare l'*indirizzo IP del* server di registrazione	Configurare il server syslog di destinazione per la registrazione dei messaggi del sistema esterno.
imposta abilitazione server di registrazione	Consentire il server di registrazione esterno.
impostazione attivazione timestamp registrazione	Attiva l'indicatore orario dei messaggi nel registro.
impostazione predefinita spantree 6 del livello di registrazione	Aumentare il livello syslog predefinito di STP.
imposta livello di registrazione sys 6 predefinito	Aumentare il livello predefinito del syslog di sistema.
imposta gravità server di registrazione 4	Consentire l'esportazione solo del syslog con un livello di gravità superiore.
impostare la console di registrazione su disable	Disabilitare la console a meno che non si esegua la risoluzione dei problemi.
set snmp community read-only *string*	Configurare la password per consentire la raccolta dati

	remota.
set snmp community read-write *string*	Configurare la password per consentire la configurazione remota.
set snmp community read-write-all *string*	Configurare la password per consentire la configurazione remota, incluse le password.
set snmp trap enable all	Abilitare le trap SNMP sul server NMS per gli avvisi di guasti ed eventi.
imposta *stringa indirizzo server* **trap snmp**	Configurare l'indirizzo del ricevitore di trap NMS.
set snmp rmon enable	Abilitare RMON per la raccolta di statistiche locali. Per ulteriori informazioni, consultare la sezione Monitoraggio remoto di questo documento.
impostare ntp broadcastclient enable	Abilitare la ricezione accurata dell'orologio di sistema da un router upstream.
imposta *nome fuso* **orario ntp**	Impostare il fuso orario locale per il dispositivo.
imposta *dettagli modifica data ora* **estiva ntp**	Configurare l'ora legale se applicabile per il fuso orario.
impostazione autenticazione ntp abilitata	Configurare le informazioni temporali crittografate per motivi di sicurezza.
set ntp key *key*	Configurare la chiave di crittografia.
set cdp enable	Verificare che l'individuazione dei router adiacenti sia abilitata (abilitata anche sulle porte per impostazione predefinita).
impostare l'*indirizzo IP* **primario del server tacacs**	Configurare l'indirizzo del server AAA.
impostare l'*indirizzo IP del* **server tacacs**	Server AAA ridondanti, se possibile.
imposta tentativi tacacs 3	Consentire 3 tentativi di password per l'account utente AAA.
imposta *chiave* **tacacs**	Impostare la chiave di crittografia AAA MD5.
impostazione del timeout di tacacs 15	Consente un timeout del server più lungo (cinque secondi sono l'impostazione predefinita).
imposta tacacs di	Usare AAA per l'autenticazione

accesso autenticazione per abilitazione	per l'accesso.
set authentication enable tacacs enable	Usare AAA per l'autenticazione della modalità abilitazione.
impostazione accesso autenticazione locale abilitazione	Predefinito; consente il fallback a locale se non è disponibile alcun server AAA.
impostazione autenticazione abilitazione locale abilitazione	Predefinito; consente il fallback a locale se non è disponibile alcun server AAA.

Comandi di configurazione delle porte host

Comando	Commento
set port host *port range*	Rimuovere l'elaborazione della porta non necessaria. Questa macro imposta l'abilitazione Spantree PortFast, la disattivazione del canale e la disattivazione del trunk.
imposta *intervallo porte* disabilitate udld	Rimuovere l'elaborazione delle porte non necessaria (disabilitata per impostazione predefinita sulle porte in rame).
set port speed *port range* auto	Utilizzare la negoziazione automatica con driver NIC host aggiornati.
set port trap *port range* disable	Nessuna necessità di trap SNMP per gli utenti generici; tenere traccia solo delle porte principali.

Comandi di configurazione del server

Comando	Commento
set port host *port range*	Rimuovere l'elaborazione della porta non necessaria. Questa macro imposta l'abilitazione Spantree PortFast, la disattivazione del canale e la disattivazione del trunk.
imposta *intervallo porte* disabilitate udld	Rimuovere l'elaborazione delle porte non necessaria (disabilitata per impostazione predefinita sulle porte in rame).
set port speed *port range 10 | 100*	Configurare in genere porte statiche/server; in caso contrario, utilizzare la negoziazione automatica.

set port duplex *port range* ***full | metà***	Generalmente porte statiche/server; in caso contrario, utilizzare la negoziazione automatica.
set port trap *port range* **enable**	Le porte del servizio chiave devono inviare trap al sistema NMS.

Comandi di configurazione delle porte inutilizzate

Comando	Commento
impostare spantree portfast *port range* disable	Abilitare l'elaborazione e la protezione delle porte necessarie per STP.
set port disable *port range*	Disabilitare le porte inutilizzate.
impostazione *intervallo porte vlan fittizie inutilizzate*	Indirizzare il traffico non autorizzato alla VLAN non utilizzata se la porta è abilitata.
imposta *intervallo porte* **trunk su disattivato**	Disattivare il trunking della porta fino alla sua amministrazione.
impostare la modalità *intervallo porte* **canale su off**	Disabilita il channeling della porta fino alla sua amministrazione.

Porte dell'infrastruttura (switch-switch, switch-router)

Comando	Commento
set udld enable *port range*	Abilita il rilevamento dei collegamenti unidirezionali (non predefinito sulle porte in rame).
imposta *intervallo porte* **di abilitazione modalità aggressiva udld**	Attiva modalità aggressiva (per i dispositivi che la supportano).
set port negoziazione *port* range enable	Consente la negoziazione automatica GE predefinita dei parametri di collegamento.
set port trap *port range* **enable**	Consenti trap SNMP per queste porte chiave.
imposta *intervallo porte* **trunk su disattivato**	Disattivare la funzionalità se non si utilizzano i trunk.
set trunk *mod/porta ISL desiderato | dot1q | negoziare*	Se si utilizzano trunk, è preferibile utilizzare dot1q.
cancella	Limitare il diametro dell'STP

***intervallo vlan mod/porta* trunk**	eliminando le VLAN dai trunk in cui non sono necessarie.
impostare la modalità *intervallo porte* canale su off	Disattivate la feature se non utilizzate i canali.
impostare la modalità *intervallo porte* canale desiderabile	Se si utilizzano i canali, PAgP viene attivato.
set port channel all distribution ip both	Consente il bilanciamento del carico di origine/destinazione L3 se si utilizzano canali (impostazione predefinita su Catalyst 6500/6000).
set trunk *mod/porta ISL* non negoziata / *dot1q*	Disabilitare il DTP in caso di trunking su router, Catalyst 2900XL, 3500 o altro fornitore.
set port negotiation *mod/porta* disable	La negoziazione può essere incompatibile per alcuni dispositivi GE meno recenti.

Informazioni correlate

- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 4500/4000
- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 5000/5500
- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 6500/6000
- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems